



Nortel Business Communications Manager 450 1.0

Planning and Engineering

Release 1.0

Document Revision 01.01

NN40160-200

Document status: Standard
Document issue: 01.01
Document date: August 2008
Product release: BCM450 1.0
Job function: Planning and Engineering
Type: Publication
Language type: EN

Copyright © 2008 Nortel Networks.
All Rights Reserved.

NORTEL, the globemark design, and the NORTEL corporate logo are trademarks of Nortel Networks.

Contents

New in this release	11
Line configuration	11
Dialing plans	11
Voice messaging and centralized voice mail	12
VoIP configuration	12
DHCP configuration	12
CLID configuration	12
Introduction	13
Line configuration overview	15
Target line configuration	15
PRI line configuration	16
T1-loop start trunk configuration	16
T1-DID line configuration	17
T1-digital ground start line configuration	17
T1-E&M line configuration	18
DASS2 line configuration	18
DPNSS line configuration	18
Line planning overview	21
Line planning prerequisites	21
How the system identifies lines	21
Line programming identification	22
ISDN BRI loop properties	25
BRI loop types and general parameters	25
ISDN BRI T-loops	26
ISDN BRI S-loops, lines, and devices	27
Calling line identification	29
Name display	29
Scope of CLID	30
CLID and business name display	31
Alpha-tagging for name display	31
CLID on incoming VS outgoing calls	31

CLID for outgoing ISDN and VoIP calls 32

Dialing plan set-up 35

BCM450 dialing plans 35

BCM450 incoming-call processing 37

BCM450 dialing plans 37

Basic numbering and access codes 39

Routing for outgoing calls 42

Routing for incoming calls 44

BCM450 access codes 45

Call routing configuration 51

BCM450 call-by-call services 52

BCM450 destination codes 56

Dialing plan and routing configurations 63

Configuration prerequisites for dialing plans 63

Destination coding in a network 63

Destination codes and code grouping 64

Dialing plan—routing and destination codes 67

Dialing plan route configuration 67

PRI route types 71

Dialing plan destination code configuration 71

Dialing plan alternate routing schedules 73

Second dial tone for outgoing PRI 74

Dialing plan configuration for public network 77

Public dialing plan settings 77

Public network settings 77

Public network DN lengths 80

Outgoing public calls routing 81

Carrier code settings 82

Dialing plan configuration for private networks 83

Private network dialing plan configuration 83

Outgoing private calls routing 89

Dialing plan configuration for line pools and access codes 91

Line pools and access codes for dialing plans 91

Potential line pool number conflicts 93

Line pools and DNs 93

Line pool call-by-call limits (PRI) 94

Private networking—basic parameters 97

Types of private networks 97

Keycode requirements 99

Dialing plan system-level settings	101
Dialing plan global settings	101
DN length configuration constraints	104
Public networking—tandem call from private node	107
Tandem calls from a private node	107
Caller access on a tandem network	109
Private networking—MCDN over PRI and VoIP	111
MCDN used to network with Meridian	111
MCDN call features over PRI SL-1 lines	113
UDP-specific programming	116
CDP-specific programming	117
Meridian 1 programming	118
Fallback over VoIP MCDN	119
Networking with ETSI QSIG	120
Private networking—MCDN and ETSI network features	123
MCDN network features	123
ETSI Euro network services	123
Private networking—PRI and VoIP tandem network	125
PRI and VoIP tandem configurations	125
Call progress through tandem networks	127
VoIP to tandem systems	130
Example of a private network configured for fallback	132
Private networking—DPNSS network services (UK)	135
DPNSS diversion feature	135
DPNSS redirection feature	137
Executive intrusion	137
Call offer	138
Route optimization	139
Loop avoidance	140
Private networking with DPNSS	140
Private network—Destination codes	145
Destination codes in BCM450	145
Private networking—PRI call-by-call services	149
PRI call-by-call services	151
Benefits of call-by-call services	151
Voice messaging	155
Centralized voice messaging (ext mail)	155
Local vox msg access (CallPilot)	157
Silent record-a-call network storage locations	158

Centralized voice mail	159
Voicemail with local system as host	159
Prerequisites for configuring voicemail	160
Configuration levels	160
Host impacts on VoIP networking	161
VoIP overview	163
Uses for VoIP	163
Key VoIP traffic concepts	163
IP telephones in VoIP network	165
VoIP trunk gateway configuration	169
DTMF handling using RFC2833	169
SIP proxy configuration	170
Configuration for SIP authentication	170
VoIP trunk gateways	173
Uses for VoIP trunk gateways	173
Prerequisites for VoIP trunk gateway configuration	174
Local gateway programming	175
VoIP routing table	177
PSTN access to a remote node	177
Fallback to PSTN from VoIP trunks	178
Scope of optional VoIP trunk configurations	181
VoIP trunks for fallback configuration	187
Prerequisites for trunk fallback configuration	187
VoIP interoperability—gatekeeper configuration	189
CS1000 as a gatekeeper	189
CS 1000 configuration	190
Private network—MCDN over PRI and VoIP specifications	191
MCDN networking checklist	191
Example of private network with Meridian 1	192
Module programming for example	193
MCDN dialing plan settings	193
Network routing information	193
Example of ETSI QSIG networking	195
Hardware parameters for example	195
T.38 fax	197
Prerequisites for T.38 fax configuration	197
T.38 Fax operational parameters	197
T.38 Fax restrictions	198
SIP fax over G.711	199
Prerequisites for SIP G.711 configuration	199

SIP G.711 operational parameters	199
SIP G.711 restrictions	200
Meet Me Conferencing	201
Prerequisites for Meet Me Conferencing configuration	201
System configuration for Meet Me Conferencing	202
Ports overview	207
RTP over UDP and its uses	207
UDP and its uses	207
Signaling ports and its uses	207
Media gateway overview	209
Media gateways	209
Media Gateways panel	211
Media Gateways panel	211
Call security and remote access	213
Call security and remote access	213
Programming for remote call-in	216
Remote access packages definitions	219
CoS and DISA	220
External access tones	221
DISA configuration for call security	223
Remote access control	223
Remote access control configuration	224
Configuration for a PRI trunk	225
Additional configuration programming	226
Restriction filters for call security	231
Restriction filters for call security	231
Remote access packaging configuration	233
Remote access packaging configuration	233
LAN overview	235
Definition and scope of a LAN	235
LAN configuration parameters	235
LAN DHCP configuration	235
Line configuration planning	237
Defining line pools	237
BCM as a DHCP client	239
BCM as a DHCP client	239
Data networking overview	241
Data networking	241

BCM VoIP capability	241
Configuration for BCM in data networking	241
BCM IP sub-system configuration	243
BCM IP sub-system configuration	243
Data network prerequisites checklist	245
Network diagram creation checklist	245
Network assessment checklist	246
Required keycodes checklist	246
System configuration for IP telephone functions checklist	247
VoIP trunks checklist	247
IP telephone records checklist	248
DHCP configuration	249
DHCP server general settings tab	249
IP Terminal DHCP Options tab	251
Address ranges tab	254
Lease information tab	255
VLAN overview	257
Overview to virtual LANs	257
DHCP and VLAN	258
Site-specific options for VLAN	258
DHCP overview	259
DHCP context in BCM450	259
DHCP default configuration	260
DHCP server on the Main Module	260
Dial Up overview	261
Remote access service	261
Automatic data dial-out service	263
Modem compatibility	264
ISDN planning and engineering	265
ISDN standards compatibility	265
ISDN network planning	265
Ordering ISDN PRI	265
Ordering ISDN BRI	266
Supported ISDN protocols	267
Setting up a dialing plan	269
Planning the use of destination codes	269
Private network—PRI and VoIP tandem network specifications	271
Example private tandem network of BCMs	271
Destination codes, external terminating calls	271

Dialing plan and routing specifications	273
Destination code leading digits	273
Meridian 1 access versus BCM access codes	273
Routing service record, public line pool	274
Routing service record, destination code	274
Tandem call progression	275
Dialing plan—routing and destination codes specifications	277
Destination codes schedules	277
Second dial tone values and descriptions	278
Private network—DPNSS network services (UK) specifications	279
Example of Private network with DPNSS	279
Calling number values for network example	280
Routing description for network example	280
Guidelines for private DPNSS network dialing plan	281
VoIP trunk gateway specifications	283
T.38 fax protocol restrictions and requirements	283
Example of call flow, PSTN into remote node	283
Detail of call progress for example	284
Example of a fallback network	285
Gatekeeper call scenarios	286
Detail of call progression for example	287
SIP fax over G.711 specifications	289
G.711 Fax restrictions	289
Operational notes and restrictions	290
T.38 fax specifications	291
Example of private network configured for T.38 fax	291
Programmed Media gateway values for example	291
Voice messaging specifications	293
Default VoIP settings specifications	295
BCM450 models	295
Call security and remote access specifications	297
Default restriction filters	297
Default filters for program headings	298
External access tones, definitions	298
Example of line restriction	298
Call progress through restrictions	299
Example of remote line restriction	299
Call progress through restrictions	299

CoS password configuration for remote access specifications
301

Example of CoS to access system over PSTN 301

Example of CoS to bypass filters on a set 301

Dialing plan specifications **303**

System identification of calls 303

Default access codes 304

Tips on using access codes 304

Protocols that support call-by-call limits 305

Available call-by-call services 305

Switches supporting call-by-call limits 306

PRI service type / DN type values for BCM450 307

PRI service type / Service ID description 307

New in this release

The following section gives a brief overview of BCM450 features described in this guide.

Navigation

- [Line configuration \(page 11\)](#)
- [Dialing plans \(page 11\)](#)
- [Voice messaging and centralized voice mail \(page 12\)](#)
- [VoIP configuration \(page 12\)](#)
- [DHCP configuration \(page 12\)](#)
- [CLID configuration \(page 12\)](#)

Line configuration

Review these sections for information on planning concepts for configuring lines and trunks on the BCM450, including target lines and PRI lines. For more information, see the following chapters:

- [Line configuration overview](#)
- [Line planning overview](#)

Dialing plans

Review these sections for planning information and prerequisites for configuring flexible dialing plans using access codes, destination codes, PSTN trunks, and private network trunks that provide multiple options for customizing your dialing options.

For more information, see the following chapters:

- [Dialing plan set-up](#)
- [Dialing plan and routing configurations](#)
- [Dialing plan—routing and destination codes](#)
- [Dialing plan configuration for public network](#)
- [Dialing plan configuration for private networks](#)
- [Dialing plan system-level settings](#)

Voice messaging and centralized voice mail

Review these sections for information and prerequisites for configuring voice messaging and centralized voice mail for your system.

For more information, see the following chapters:

- [Voice messaging](#)
- [Centralized voice mail](#)

VoIP configuration

Review these sections for information and prerequisites for configuring VoIP trunks to establish communications between a BCM and a remote system across an IP network. The BCM450 supports both SIP trunks and H.323 trunks.

For more information, see the following chapters:

- [VoIP overview](#)
- [VoIP trunk gateway configuration](#)
- [VoIP trunk gateways](#)
- [VoIP trunks for fallback configuration](#)
- [VoIP interoperability—gatekeeper configuration](#)

DHCP configuration

Review the following sections for information and prerequisites on how to use Dynamic Host Configuration Protocol (DHCP) to reduce the complexity of configuring IP devices, particularly IP phones. Through DHCP, IP phones receive an IP address as well as additional information such as gateway and port information.

For more information, see the following chapters:

- [DHCP overview](#)
- [DHCP configuration](#)

CLID configuration

Review planning information and prerequisites for configuring calling line identification (CLID) for incoming and outgoing calls.

For more information, see the following chapter:

- [Calling line identification](#)

Introduction

This document contains conceptual and reference information for planning the configuration for your Business Communications Manager 450 (BCM) system. This guide is intended for network planners. For network configuration procedures, see *Nortel Business Communications Manager 450 1.0 Configuration—Telephony* (NN40160-502).

The information in this guide describes planning concepts for topics such as

- private and public networks configuration
- dialing plan configurations
- voice messaging and centralized voice mail configuration
- T.38 fax
- SIP G.711
- ports
- media gateways
- call security
- DISA
- VoIP
- Meet Me Conferencing
- data networking

The information in this guide provides reference material for topics such as

- private networking basic parameters
- dialing plan outgoing destination codes
- dialing plan routing
- T.38 fax
- SIP G.711
- default VoIP settings
- firewall configuration resources

14 Introduction

- call security remote access
- CoS password specifications
- dialing plan specifications

Line configuration overview

This section provides an overview of line configuration.

Telephony signals into the system, within the system, and out of the system are carried over channels. For consistency, these channels are all called lines or trunks. This designation includes

- circuit switched lines (PSTN): connect to the system through media bay modules
- Voice over IP (VoIP) trunks: connect through the LAN or IP network
- target lines, internal channels: connect PRI, T1 and VoIP trunks to specific devices
- intercom lines: connect all internal telephones together through the DN numbers, and allow the user to access line pools for making outgoing calls, as well as being required for other call features such as conference calling and system-wide call appearance (SWCA) calls.
Intercom designations are assigned in the DN record, or automatically by the system for each telephone.

Target line configuration

Target lines are virtual lines that allow the mapping of received digits to a line number over PRI channel.

The following paths indicate where to access target lines in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Lines > Target Lines**
- Telset interface: ****CONFIG > Lines**

Configuration prerequisites for target lines

Complete the following prerequisites checklist before configuring the modules

Install and configure the DTM module.	
Provision lines.	

PRI line configuration

PRI are auto-answer lines. These lines cannot be individually assigned to telephones. They must be configured into line pools. PRI line pools then are assigned routes and these routes are used to create destination codes.

The following paths indicate where to access PRI line pools in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Lines**
- Telset interface: ****CONFIG > Lines**

Configuration prerequisites for PRI lines

Complete the following prerequisites checklist before configuring the modules.

Install and configure the DTM module.	
Provision lines.	

PRI line features

The services and features provided over PRI lines include

- Call-by-call service selection (NI protocol)
- Emergency 911 dialing, internal extension number transmission
- access to Meridian 1 private networking (SL-1 protocol)

T1-loop start trunk configuration

Loop start trunks provide remote access to the BCM from the public network. They must be configured to auto-answer to provide remote system access. A loop start trunk must have disconnect supervision if it is to operate in the auto-answer mode.

The following paths indicate where to access the loop start trunks information through Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Lines**
- Telset interface: ****CONFIG > Lines**

Configuration prerequisites for T1-loop start

Complete the following prerequisites checklist before configuring the modules.

DTM module is installed and configured.	
---	--

T1-DID line configuration

DID (Direct Inward Dial) are lines on a digital trunk module on a T1. Inbound DID lines are mapped through target lines.

The following paths indicate where to access the DID lines in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Lines**
- Telset interface: ****CONFIG > Lines**

Configuration prerequisites for T1-DID lines

Complete the following prerequisites checklist before configuring the modules.

DTM module is installed and configured.	
---	--

Lines are provisioned.	
------------------------	--

T1-digital ground start line configuration

The following describes how to configure digital Ground Start lines.

The following paths indicate where to access the Ground Start lines through Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Lines**
- Telset interface: ****CONFIG > Lines**

Configuration prerequisites for T1-digital ground start

Complete the following prerequisites checklist before configuring the modules.

DTM module is installed and configured.	
---	--

Lines are provisioned.	
------------------------	--

T1-E&M line configuration

E&M lines must be digital (T1).

The following paths indicate where to access the E&M lines in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Lines**
- Telset interface: ****CONFIG > Lines**

Configuration prerequisites for T1 E&M lines

Complete the following prerequisites checklist before configuring the modules.

DTM module: Installed and configured.	
Lines are provisioned.	

DASS2 line configuration

DASS2 trunks are specific to the UK market.

The following paths indicate where to access the DASS2 trunks in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Lines**
- Telset Interface: ****CONFIG > Lines**

Configuration prerequisites for DPNSS lines

Complete the following prerequisites checklist before configuring the modules.

DTM module is installed and configured.	
Lines are provisioned.	

DPNSS line configuration

DPNSS trunks are used in all international markets.

The following paths indicate where to access the DPNSS trunks in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Line**
- Telset Interface: ****CONFIG > Lines**

Configuration prerequisites for DPNSS lines

Complete the following prerequisites checklist before configuring the modules.

DTM module is installed and configured.	
Lines are provisioned.	

Line planning overview

The chapter [Line configuration overview \(page 15\)](#) provides an overview of line configuration concepts. This chapter discusses planning concepts for line configuration, including defining line numbers and destination codes, and defining line pools.

Line planning prerequisites

You must configure the media bay modules or the VoIP trunk parameters, or both, before you can set up line programming.

- The position on the system bus of the trunk media bay modules determines the line numbers that are available.
- The position on the system bus of the station media bay modules determines which DNs are available, although DN numbers can be changed.
- The BCM450 supports 48 IP trunks, and up to 130 trunks with the capacity expansion card (CEC) installed. Available VoIP lines are determined by the number of VoIP keycodes entered on the system (between 1 and 130).

Other line configuration options or requirements include

- BRI loops require configuration and provisioning before the BRI lines can be configured.
- The BCM450 does not support the DDIM (digital drop insert MBM).

How the system identifies lines

On a new system, lines and loops are numbered and assigned defaults based on the type of media bay modules that have been connected to the system. The exception are the VoIP trunks, which require a keycode to activate.

These panels allow you to easily view which lines have been enabled through a media bay module. From this heading, you can access each line record and assign attributes, as you require.

Line programming identification

Under Lines, note that line types are divided into five headings. The fifth heading contains all line numbers.

- Active physical lines
- Active VoIP lines (require keycode)
- Target lines
- Inactive Lines
- All Lines

Active physical lines

You can configure up to 150 physical lines.

Active VoIP lines (require keycode)

Voice over IP (VoIP) lines are signaling channels that simulate how CO lines work. However, VoIP lines transmit data to the IP network over a LAN or IP network rather than over physical lines. Once the VoIP trunks are set up, you can assign them to line pools, and program their behavior in the same way you would PRI lines.

The BCM450 supports 48 IP trunks, and up to 300 lines with the capacity expansion card (CEC) installed. These line records appear under Configuration > Telephony > Lines > Active VoIP Lines. To access VoIP lines, you need to enter software keycodes. Each keycode supports a specific number of lines. No entries appear in the Enabled VoIP lines field until you complete the IP Trunks Settings field, which appears when you click IP Trunks under Configuration > Resources > Telephony Resources > IP trunks.

VoIP trunks should be configured to use a single line pool per trunk type. Do not mix other trunk types on the same line pool. The VoIP line pools are assigned to routes, which, in turn, are configured with destination codes that route calls to the designated remote gateways of other BCM systems or Succession, or MCS5100 systems.

You can also create a fallback for the trunk. This is a situation where the system reroutes the call to a PSTN line pool if the primary route is not available or the call quality is not suitable. If you do not configure your network for fallback and the call quality is below threshold, the IP call fails.

Target lines

Target lines are internal communications paths that directly connect auto-answer trunks to system telephones. These lines are incoming only.

Target lines allow you to make more efficient use of DID line resources. You can map a range of target lines for each DID line. The incoming call is routed according to the mapped dialed digits, rather than a one-to-one line assignment. Systems configured using the DID template automatically assign target lines to all assigned DNs.

You also require target lines when you use PRI, T1 or VoIP trunks. Target lines use line numbers 361 to 680. To view these lines, select Configuration > Telephony > Lines > Target Lines. Record this information in your system Programming Records so you have a clear view of where each line is assigned.

Other features: of target lines are

- Each target line can be assigned to more than one telephone.
- A telephone can have multiple appearances of a target line

Target lines are internal direct links the BCM uses to allow external callers to dial specific system telephones or a group of system telephones. You assign the target line to one or more telephone DNs, and then configure the target line to function as you require. You can also assign multiple appearances of a target line to one telephone. This allows more than one call to simultaneously use the target line. Target lines are required by lines that support multiple numbers over one trunk (T1 E&M, DID trunks, T1 DID trunks, PRI trunks, and VoIP trunks).

The following trunks use one or both of these settings to route calls:

- DPNSS lines use the Private received number to route calls in the system.
- BRI ETSI-QSIG, PRI ETSI-QSIG, MCDN, DMS-100, DMS-250, and VoIP trunks route calls on a per-call basis to either the public or private received digits.

Attention: VoIP trunking MCDN calls do not support Auto DN/DISA DN functionality.

- BRI (ETSI-Euro, NI), PRI (ETSI-Euro, NI, 4ESS), T1 (LoopStart, E&M, DID, GroundStart), Analog LEC (LoopStart), and DASS2 trunks route calls using the Public received number.

Physical lines

Physical lines are the central office (CO) trunks assigned to the trunk media bay modules.

You can change the line types to suit your system. For instance, BRI and DTM modules can be designated to a number of line types, depending on the type of line service provided through the central office (CO). However, the line numbers are associated for specific tasks or to specific DS30 bus numbers.

The line record allows you to program settings for lines that affect how the lines operate in the network and with other switches, as well as how the system uses the line.

The trunk types: are

- VoIP
- DTM (digital): TI types (Loop, E&M, DID, Ground, or fixed data channel), PRI, DASS2, DPNSS)
- CTM (North America)/GATM: Analog Loop
- BRI: BRI S/T
- target lines

ISDN BRI loop properties

This section gives an overview of ISDN BRI loop properties.

The following paths indicate where to configure loops through Element Manager and through

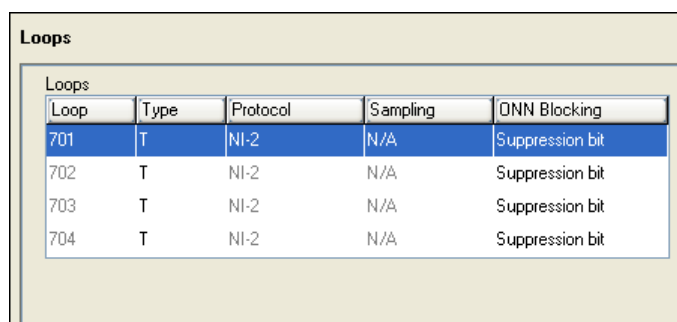
Telset Administration

- Element Manager: Configuration > Telephony > Loops
- Telset interface: **CONFIG > Hardware > Module > TrunkMod > BRI - X > Loop XXX

BRI loop types and general parameters

The Loops table displays the BRI loops for an installed module and the settings that are common to both T-loops and S-loops. The following figure illustrates the Loops table.

Figure 1 Loops table



Loop	Type	Protocol	Sampling	ONN Blocking
701	T	NI-2	N/A	Suppression bit
702	T	NI-2	N/A	Suppression bit
703	T	NI-2	N/A	Suppression bit
704	T	NI-2	N/A	Suppression bit

The following table describes the fields found on the Loop main panel. To access the Loop main panel in Element Manager, click Configuration> Telephony> Loops.

Table 1 Loops main panel

Attribute	Value	Description
Loops	<X01-X04>	Each BRI module supports four loops (eight lines for T-loop programming).
Type	T S	This setting defines whether the loop supports trunks (T-loop) or device connections (S-loop). Attention: This variable can be different for different market profiles.
Protocol	Euro QSIG NI-2	Select the appropriate ISDN protocol. The values displayed depend on both the market profile and software keycodes Euro - ETSI ISDN standard QSIG - also an ETSI standard. Only appears if the ETSI QSIG keycode is loaded NI-2
Sampling (S loops only)	Adaptive Fixed N/A	Select a sampling rate for the S-loop. Fixed: two or more S-interface devices use the loop, and the length of the loop is less than 200 m (650 ft.). Adaptive: two or more S-interface devices use the loop, and the length of the loop is greater than 200 m (650 ft.). If one device is using the loop, the length of the loop can be a maximum of 1000 m (3230 ft)
ONN blocking	Suppression bit Service code	Set the Outgoing Name and Number (ONN) Blocking. When you activate ONN, a user can press FEATURE 819 to block the outgoing name and number on a per call basis. Programming note: Ensure that all telephones that have this feature available are assigned valid OLI numbers. Refer to "Programming outgoing number display (OLI)" on page 217.

ISDN BRI T-loops

BRI modules support both trunk and station (telephone) services.

Configuring prerequisites for BRI T-loops

Complete the following prerequisites checklist before configuring the modules.

Ensure that system hardware is installed and operating correctly	
Obtain all relevant central office/service provider information for the loops.	
BRI module is installed and operating (LEDs are correct).	

ISDN BRI S-loops, lines, and devices

BRI modules support both trunk and station (telephone) services. The following describes the process for configuring station/device (S) loops, which support devices that use an ISDN interface. You can assign a single device to a loop, or multiple devices connected through an NT-1 interface.

BRI device connections: properties

BRI S-loops support devices that use an ISDN interface. For an overview of ISDN, see *Nortel Business Communications Manager 450 1.0 Installation—Devices* (NN40160-302). You can assign a single device to a loop, or multiple devices connected through an NT-1 interface.

- You can assign a maximum of eight devices to a loop.
- Any device can only be configured to one loop.
- S-loops do not supply any voltage for ISDN devices requiring power, such as video cameras. Voltage for these devices must be supplied by an external source on the S-loop.

Configuration prerequisites for BRI device connections

Complete the following prerequisites checklist before configuring the modules.

Ensure that system hardware is installed and operating correctly
Obtain all relevant central office/service provider information for the loops.
BRI module is installed and operating (LEDs are correct).
Wiring is complete for ISDN device configuration

DN records for ISDN BRI devices

ISDN telephones and devices have a limited feature set. They do not have programmable buttons or user preferences, and do not support call forward features. However, you can assign Answer DNs and some capabilities features.

Configuration prerequisites for BRI devices

Ensure that the following prerequisites checklist is complete before configuring the devices

BRI module installation and configuration is complete. For information on trunk module parameters, see <i>Nortel Business Communications Manager 450 1.0 Configuration—System</i> (NN40160-501).	
BRI loops programming is complete.	
Lines are provisioned and configured. For information on provisioning lines and loops, see <i>Nortel Business Communications Manager 450 1.0 Configuration—System</i> (NN40160-501).	
Wiring and network connections for the devices are complete.	

ISDN BRI set DN record configuration

On each panel on the DN's list, add or modify settings to customize the telephone operations. The following headings correspond to each panel. Refer to the Programming notes in each section for configurations that are unique or specific for ISDN telephones.

Table 2 ISDN device-specific DN record settings

Affected fields	Setting	Panel name and link to common procedures
Name	Unique to each device or device loop	
Call forward	Not supported	
Line appearances	Ring only	
Answer DNs	Ring only	
Intercom keys	two: not configurable	
The following settings are the only capability settings that require specific configuration for ISDN devices		
Page settings	Page only-select. Devices cannot be assigned to Page zones	If Enabled, the specified OLI for the telephone is used for CLID for calls.
OLI as called number	<check box>	
All other settings are variable, based on your system requirements		

Calling line identification

This section gives an overview of calling line identification (CLID).

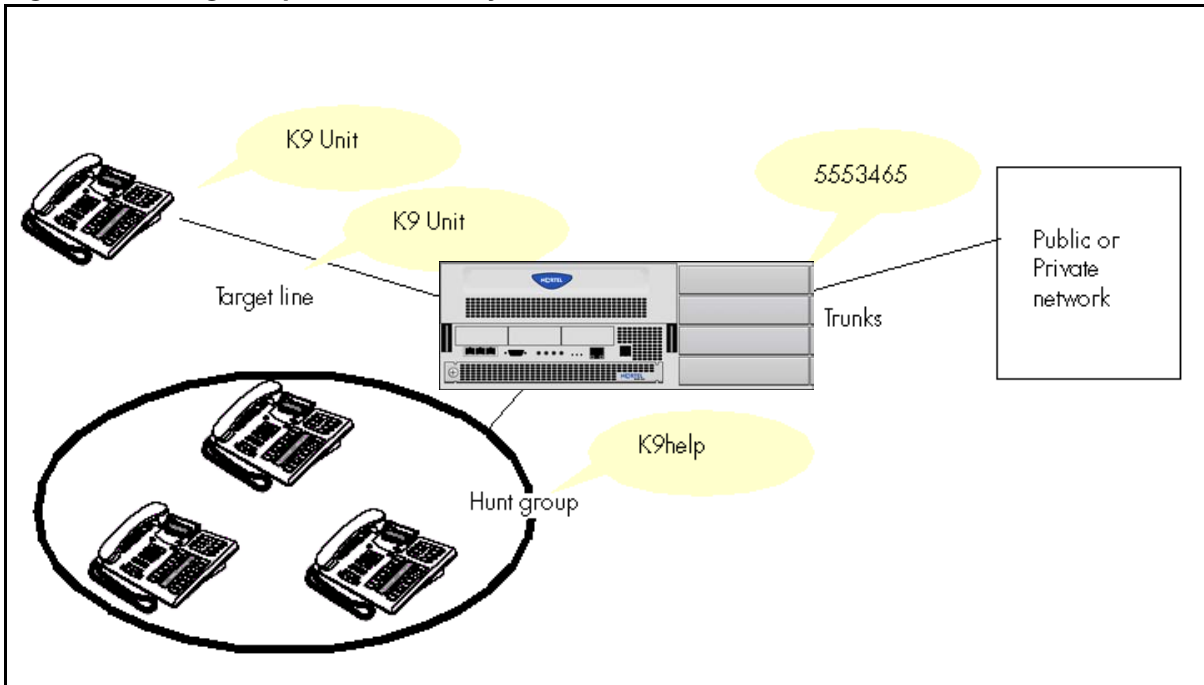
BCM displays the name of the calling party at the answering telephone when this information is available on Private or Public PRI trunks, VoIP trunks, and analog trunks that support CLID.

Name display

You can assign names to identify your company, external lines, target lines, and your colleagues' telephones. During a call, the name (if programmed) appears on the telephone display instead of on the external line number or internal telephone number of the caller. Names can contain both letters and numbers, but cannot be longer than seven characters. You cannot use the number (#) and star (*) symbols.

Attention: You can give the same name to a telephone and a line in your system. Use initials, abbreviations, or even nicknames to give each telephone a unique name to avoid confusion.

You can also determine if the CLID is received by a telephone, or if the CLID information from a system telephone gets sent out over the network. Refer to [CLID on incoming VS outgoing calls \(page 31\)](#). The following figure illustrates an example of naming system components.

Figure 2 Naming components in the system

Scope of CLID

The displayed name can include the Receiving Calling Name, Receiving Redirected Name, and/or Receiving Connected Name. Refer to [CLID transmission and receipt \(page 30\)](#). If only a number is available for CLI on an incoming call, you can program a system speed dial in such a way that a name displays when that number calls in. Refer to [Alpha-tagging for name display \(page 31\)](#).

Name and number information are also transmitted with outgoing calls. This can be blocked by the user (FEATURE 819) on a per-call basis. As well, you can block this information on a per-trunk basis. This is important if the connecting system cannot process name and number information. Some service providers also may have different codes that need to be mapped so that the blocking feature works.

CLID transmission and receipt

Network Name Display displays the name of an incoming PRI/BRI, analog with CLID, or VoIP with MCDN call on the BCM telephone receiving the call.

Calling Party Name with status of Private can appear on the Called Party telephone as Private name. If the incoming Calling Name is defined by the CO as a private name, then Private name appears on the answering telephone. If the Calling Party Name is unavailable it can appear on the Called Party telephone as Unknown name.

If the call is answered by a Hunt group, the hunt group name appears instead of the telephone name in forming the connected name.

The Connected Name is a transient display that appears for approximately three seconds. The Connected Name is sent only if the OLI is programmed. You can program both a public and private OLI. The system uses the one appropriate to the type of call.

CLID interoperability with network name display

Calling and Connected Name information (if available) passes between trunks with Selective Line Redirection (SLR). Only Calling Name information passes between trunks in cases where Direct System Inward Access (DISA) results in tandeming of trunks.

CLID and business name display

Nortel recommends that you use a blank space for the last character of the Business name to act as a separator between the Business name and telephone name. A maximum of eight characters is supported.

Alpha-tagging for name display

You can configure your system to display a caller name for incoming calls that provide number-only CLID, such as if the name service is not subscribed to or available in your area

Attention: Lines that provide name and number CLID, such as PRI lines, use that name for display, rather than the alpha tagging feature.

Limitations

- Due to system resource limitations, only 30 telephones can be assigned to provide alpha tagging CLID per line.
- If the incoming number only partially matches the CLID match length, no name displays.
- If the number matches more than one speed dial, and the matches have different names, the telephone displays the name of the first match.
- ISDN devices do not support the alpha tagging feature.

CLID on incoming VS outgoing calls

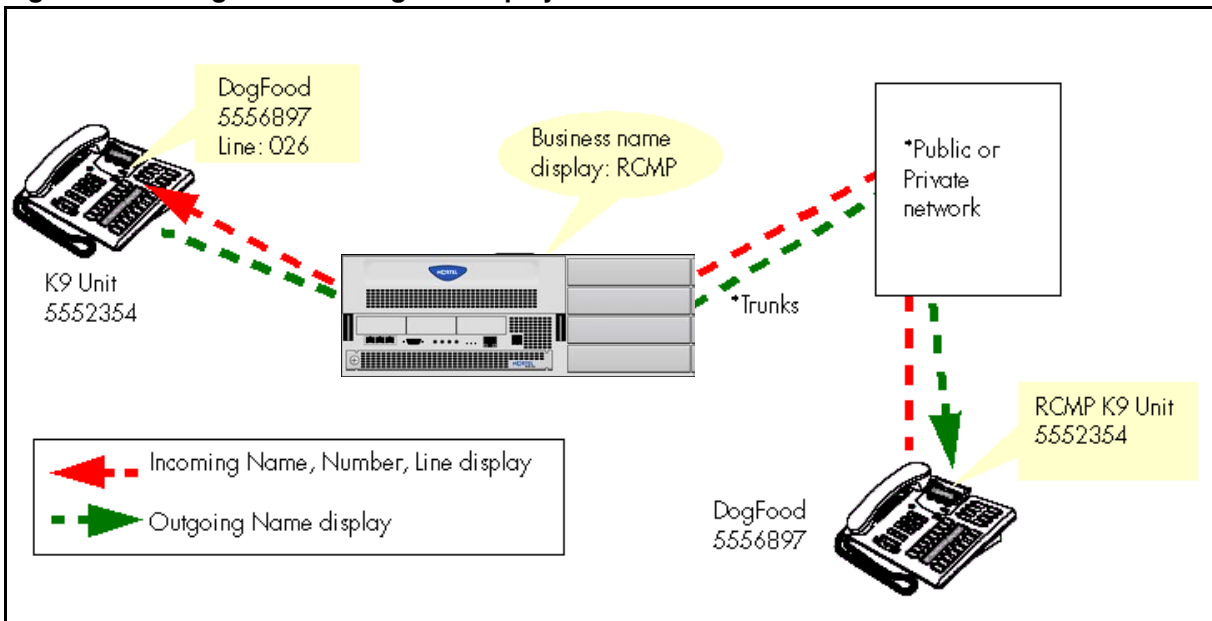
If you subscribe to Call Display services from your local telephone company, one line of information about an external caller appears on the display after you answer a call. If you answer before the Call Display information appears on your display, press FEATURE 811 to view the line number or line name.

Depending on the services you subscribe to, incoming Call Display information can contain up to three parts:

- the name of the caller
- the number of the caller
- the name of the line in your system that the call is on

Call display information can also be sent out when a system telephone calls out of the system. What displays at the called party's telephone, depends on what the private or public lines allow. Outgoing call display information can be allowed or blocked at the system level or single telephone level. The following figure illustrates an example of incoming and outgoing call display.

Figure 3 Sending and receiving call display



CLID for outgoing ISDN and VoIP calls

The Network name display feature allows ISDN to deliver the Name information of the users to those who are involved in a call that is on a public or private network.

Your system might display the name of the called party on an outgoing call, if it is provided by your service provider. Your system sends the Business Name concatenated with the set name on an outgoing call but only after the Business Name has been programmed.

With the VoIP option, CLID information received from the BCM450 server for an incoming call appears between the report header and the event lines. There is one occurrence of CLID information per call. CLID information does not appear in the report if CLID information is not available.

Attention: CDR reports CLID information only for lines that are capable of delivering CLID. Your BCM450 must have delivery of CLID information enabled.

Dialing plan set-up

This section gives an overview of the dialing plan set-up in BCM.

BCM450 dialing plans

Dialing plans allow users to access the public network, to make calls, and to answer dial strings.

Access to and from and within your system is based on dialing strings and how the system adds or deletes digits from this sequence to route the call.

Overview of dialing plans and routing

A dialing string is the numbers that the caller physically enters on a telephone or programs onto a memory key. This can also include numbers the system adds to a dial string when a call goes through call routing.

This process also includes how the receiving system reads the sequence. All of which means that coordination is required at both ends of the call to ensure that calls are routed correctly. This is especially important if calls need to be routed through your system, or through a remote system, to reach another node on the network.

Dialing plan using public lines

The following figures provide examples of how you can record dialing plan information in a spreadsheet. The example shows dialing plan information for a Toronto system in a network of three offices: Toronto, Halifax, and Vancouver. Without routing, a BCM user in Toronto must to select a line pool and dial 1-902-585-3027 to reach extension 27 in Halifax (902). By creating a destination code of 30 and creating a route that uses the proper line pool and dial out number, the user simply dials 3027. The same feature is available for Vancouver (604).

In the column Dial-out, P stands for pause, a host system signaling option. Press FEATURE 78 to insert a 1.5-second pause in the dialing string.

Figure 4 Routing service record: use pool

Routing Services (Services: Routing Service)		
Route # (000-999)	Dial-out (if required) (max. 24 digits or characters)	Use Pool
100	902-585	ABC
101	902-585	ABC
102	604-645	ABC
103	604-645	ABC

Create unique route number
 Specify dial-out digits
 Route through Pool A

Figure 5 Routing service record: Destination code

Routing service (continued)								
Dest code (Services: Routing Services: Dest Codes)								
Service Schedule	Normal		Schedule					
DestCode (max. 12 digits)	Use route (001-999)	Absorb Length	1st route (001-999)	Absorb Length	2nd route (001-999)	Absorb Length	3rd route (001-999)	Absorb Length
30	100	0	000	All	000	All	000	All
31	101	0	000	All	000	All	000	All
32	102	0	000	All	000	All	000	All
33	103	0	000	All	000	All	000	All

Create unique code Specify which route to use Add Destination code to dialout out string

BCM450 incoming-call processing

The system processes a call in the following way:

- 1 The system receives a call from the public or private network
- 2 The system identifies the call type:

Private calls:

- If the call is tagged as Private/Subscriber or Private/UDP, the system prepends the Private access code.
- If the call is tagged as Private/CDP, no access code is added.

How to determine line access dialing

[BCM450 access codes \(page 45\)](#) and [Call routing configuration \(page 51\)](#) describe what you do with the lines and loops you previously set up into line pools.

By using access codes or call routing, which uses destination codes, you can determine which lines (routes) outgoing calls use. When you create a route, you can also specify restrictions that apply to how or when the line is used.

BCM450 dialing plans

Dialing plans allow users to access the public network, to make calls, and to answer dial strings.

How dialing plans are structured

Access to and from and within your system is based on dialing strings and how the system adds or deletes digits from this sequence to route the call.

A dialing string is the numbers that the caller physically enters on a telephone or programs onto a memory key. This can also include numbers the system adds to a dial string when a call goes through call routing.

This process also includes how the receiving system reads the sequence. All of which means that coordination is required at both ends of the call to ensure that calls are routed correctly. This is especially important if calls need to be routed through your system, or through a remote system, to reach another node on the network.

Configuration for private network dialing

If your BCM is part of a private network, you have a choice of dialing plans. However, all BCMs on a network must use the same type of dialing plan and have the same Private DN lengths to ensure proper call direction. Plan these settings before you start programming for the private network.

- UDP (Universal Dialing Plan) uses a destination code and a location code plus the set DN (that is, 6-403-XXXX) to determine where a call gets routed. You specify a Private DN length to allow all required digits to be dialed. Each node on the network has a unique location code
- CDP (Coordinated Dialing Plan) uses a unique steering code that is transparent to the user and is dialed as part of the destination set's DN (that is, 2XXXX for one node, 3XXXX for another node, and so on) to determine where the call gets routed. Since each node on the network has a unique code, no other routing is required
- The Meridian system administrator, or the call control system, generates the Private Network IDs. These IDs are unique to each node on a network. Both UDP and CDP must include this code in programming.

Configuration for public network dialing

The public network settings allows you to enter DN lengths for the networks the callers are allowed to dial, including special numbers such as 411 and 911.

The public DN lengths table is used for all PRI calls except for those routes that use service type Private or service type TIE with DN Type specified as Private. This table allows the BCM to determine the length of a DN, based on the initial digits dialed.

A set of default Public DN lengths is included with the default template. In most cases it is not necessary to change the default values.

Public network DN lengths

In the public DN lengths table:

- You can define up to 30 entries.
- Each entry consists of a DN prefix string (1 to 10 digits) and a length value (two digits, 1 to 25)
- Several entries are predefined in the North America profile. These defaults can handle most regions in North America without the need for additional programming. If required, you can remove or modify these entries
- The table always contains one default entry. You cannot remove this entry. You can only modify the length parameter associated with this entry. The default entry specifies the length of any dialing string that does not match one of the other table entries.

Configuration for public and private received length

If you change the received number length for your system, the Public number entry for the target lines clear if the new received # length is less than the number entered in this field.

If the new received number length has more digits than the number entered in the target lines Public Number field, the entry remains, but does not update to the new DN length.

A private OLI is automatically assigned to the DNs if the DN length and the Received number length are the same. If either changes so that they are not the same, the private OLI field is cleared or not assigned (PBX template).

Basic numbering and access codes

This section describes basic number and access codes.

Basic numbering in the dialing plan

The first numbering of your set is your DN length (Start DN length) and Start DN and Public and Private Received # length. Start DN information is entered when the system is initially set up. These numbers can be changed after the system has been set up, but only at the risk of compromising other numbering in the system. If your system is part of a network, these numbers must be coordinated with the other nodes in the network to ensure that the network dialing plans are consistent. The Public and Private Received Number lengths take their sequence from the initial DN length, but this can be changed to accommodate local dialing requirements, the Private length should mirror the DN length, except in special circumstances.

Variable	Example settings
Start DN	221
DN length, Received # length	
Private length	3
Public length (max)	12 (North America)

Codes for remote access

When you set up lines that do not offer DISA directly on the line, you can determine if remote access prompts with DISA or allows auto answering. This determines the Public/Private Auto DN and Public/Private DISA DN settings, which are set under Configuration > Telephony > Dialing Plan > Public Network and Private Network. These numbers have the same first number as you specified in the Start DN and be of the same length. Remote callers dial the system public or private access number, and then dial either the Private/Public Auto DN or Private/Public DISA DN, as determined by the line setup.

Variable	Example or default settings
Private Auto DN	2XX
Public Auto DN	2XX
Private DISA DN	2XX
Public DISA DN	2XX

Codes for incoming calls

The Private Dialing Plan provides the special codes that identify the system to calls coming over private PSTN or VoIP trunks. Calls that do not match the private dialing plan information, are not accepted by the system.

Variable	Example or default settings
Private network ID	Number that identifies the system as part of the private network
Location code	UDP networks
Private DN length	DPNSS systems only

Calls coming in over private networks or PRI/BRI termination target lines can be set up for each telephone or group of telephones to which the calls are directed. As with other incoming calls, these calls can have a public or private call type that matches to a public or private received number assigned to a target line.

Variable	Example of default settings
Private received number	<CDP: same as DN of telephone> <UDP: LOC code + DN>
Public received number	<North America: 10 digits XXX-XXX-XXXX, the trailing digits are the DN> <DPNSS: maximum number of digits in local dialing pattern>

Codes for outgoing calls

Other network codes include the information about public dialing codes that you enter under Configuration > Telephony > Dialing Plan > Public Networks.

The public dialing plan defines which dialing string prefixes are allowed over the public PSTN lines. By defining these dial strings and the length of the prefix, the central office can direct the calls to the correct public destination.

Variable	Example of default settings
Public DN lengths (prefixes)	Public dialing table

For private networks, if you are not using routing and destination codes, you need to identify an access code that indicates an incoming call is destined for the private network.

Variable	Example or default settings
Private Access Code	6

Codes for MCDN special call types

If your system is networked to other types of systems, such as Meridian 1, which sends calls through one or more BCM systems to the public network, you need to specify specific call-type codes. These codes append to the incoming dial string, so that the call-type remains intact as it passes through the BCM call processing.

Variable	Example or default settings	
Local Access Code	9	Coordinate these settings with Meridian
National Access Code	61	routing for these calls types and the
Special Access Code	911	National Access Code 61 Private Access Code.

Line pool and destination access codes

Once the basic numbers have been picked, you can decide what numbers to use for line pool access codes and/or destination codes. The system does not allow these codes to start with any of the numbers currently assigned. If you are working with an established dialing plan, you may want to ensure that the numbers that the users are familiar with dialing are reserved for these codes.

For instance, if the users are familiar with dialing 9XXXXXXX to access numbers outside of their own offices, you must reserve this number for the destination codes. Note users get a Second Dial Tone (SDT) after pressing 9. If you are setting up a new system, you could opt to use the location codes of the other systems as destination codes, or you could define one number for local calls (but which are still outside the system) and one number for long-distance calls. For example: The users can dial 6<DN number> for calls within a local system, but dial 8<area code><office code><extension or "DN"> for calls in another city over the public network.

Variable	Example or default settings
Line pool codes (first character)	5
Destination codes (first character)	6<up to 11 more characters> 9<up to 11 more characters>

Routing for outgoing calls

Outgoing calls require line pool access codes or destination code (with defined routes) to leave the system.

- Access codes provide direct, unscheduled access to an analog, digital (T1).
- Destination codes also provide access to line pools, but they also allow more flexibility in dialing, which allows for more complex routing options, such as scheduling, fallback routing (VoIP trunks), call definition, and multiple routing (least-cost routing). Routing also allows you to minimize the dialout for the user, especially to systems on the same private network.

Routing, outgoing BCM450 calls

Outgoing calls can be either public or private, which is defined by the route. The public or private designation determines which dialing plan is used to determine the validity of the call. Normally, public calls are routed over PSTN trunks and private calls are routed over a private network. However, MCDN trunks can also pass calls designated as public to allow remote nodes on the network to call out of the PSTN of a local node. This is called tandem dialing.

- If the outgoing call is designated as private, the system checks the beginning of the string for a destination code that routes to a private network. It also checks that the dial string is the correct length. The destination code routing determines what the final dial string will be, adding or removing digits, as required.
- If the outgoing call is designated as public, the system checks the beginning of the string for a destination code that routes to a PSTN or an MCDN trunk. If the call routes to a public route, the system checks the public dialing table to ensure that the dialout string has legitimate leading digits and is the correct length. If the call routes to an MCDN trunk, the call is passed as dialed, minus the private networking codes. The call passes through the system until the system with the matching destination code receives it, at which point it is sent through the local PSTN of that system.

How the system identifies the call depends on the type of trunk chosen for the route. Refer to the table below.

Dialing plan setting	NPI/TON	Private called number length based on
MCDN trunks send private calls in this way:		
None	Private/Subscriber	Private DN length (set on Private Network panel)
UDP	Private/UDP	private access code + home location code (LOC) + private received digits
CDP	Private/CDP	private received digit
DMS-100/DMS-250/ETSI-QSIG trunks send private calls in this way:		
None	Private/Subscriber	Private DN length (set on Private Network panel)
UDP	Private/Subscriber	private access code + home location code (LOC) + private received digits
CDP	Private/Subscriber	private received digit

Routing, outgoing public calls

Outgoing public calls from within the system typically have the routes set to Public. Refer to [Call routing configuration \(page 51\)](#). The NPI/TON gets sent as Unknown/Unknown. The public called number length is based on the Public DN lengths table in the Public networks dialing plan.

MCDN trunks also allow public call types when tandeming calls from another system on the private network. Some of these systems use specific call types that the BCM needs to recognize to pass on correctly. Also refer to [Codes for MCDN special call types \(page 41\)](#).

Type of call	NPI/TON	BCM prepend access code	BCM monitor display
Local	E164/Local	Local access code(9)	E.164/Subscriber
National	E164/National	National access code (X1)	E.164/National
Special calls (international, 911, etc.)	Private/Special	Special access code (9)	

Routing for incoming calls

Incoming call routing also depends on the call type. The system also uses the Public and Private DN length settings to determine call routing.

Public DN length relaxation and impacts

The DN lengths setting allows you to change the number of digits for the Received number length and the DN length, which are used by the system to determine if an incoming call is valid for the system.

Each increase in length adds the digit 2 in front of any existing DN. For example, if DN 234 was increased to a length of four, the new DN would be 2234.

Attention: Do not change DN length immediately after a system start-up. You must wait until the system is operational with two solid green status LEDs.

Attention: Increasing the DN length affects other areas of the system: direct-dial digit, or any line pool access code, the setting for the prefix or code changes to the DN length change creates a conflict with the Park prefix, external line access code.

Attention: Optional applications affected by DN length changes: Voice mail and Contact Center applications are reset if you change the DN length after these services are installed. If you increase your DN length and then decide to decrease the DN length you must cold start your system and lose all of the programming.

Attention: If your system is running with a PBX telephony template, the Public and Private received # length are by default 3 (digits) at startup. Increasing the DN length after system startup does not change these digits, so you must manually change the Public and Private Receive Number length. Private OLI's are automatically assigned to the DN records if the DN length and the Private Received Number length are the same. If this changes, the Private OLI's are cleared, or are not assigned (PBX template). Network note: If your system is part of a private network, ensure that you confirm the dialing plan for the network before changing this length. If you change the length, ensure that you check all DN-related settings after the change.

Received number length and impacts

If you change the DN length of your system, you may need to change the Received # length. Private and public networking, and the access codes to determine a route for an incoming call over an auto-answer trunk.

On systems running the DID telephony template, the Private and Public Received # length is set to the same length as the DN length for the system. On systems running the PBX telephony template, the Private and Public Received # length default to 3, unless the DN length is changed during the Startup procedure.

These digits identify target lines ([BCM450 incoming-call processing \(page 37\)](#)), Auto DN's, and DISA DN's.

The received number can be shorter if network or central office constraints require this. This number cannot be greater than the system DN length on a networked system using a coordinated dialing plan (CDP) or a universal dialing plan (UDP). On a standalone system it is possible that the received number length would be greater than the DN length.

Attention: Decreasing the received number length clears all programmed received digits that are longer than the new settings.

BCM450 access codes

This section describes BCM450 access codes.

Park prefix

The Park prefix is the first digit of the call park retrieval code that a user enters to retrieve a parked call. If the Park prefix is set to None, calls cannot be parked.

Attention: If this field is set to None, the system-wide call appearance (SWCA) feature does not work.

Interaction of call park codes

When you park a call (FEATURE 74), the system assigns one of 25 codes for the retrieval of the call. You can then press the Page display key to announce the code that appears on the display.

These three-digit codes include the Call Park prefix, which can be any digit from 1 to 9, and a two-digit call number between 01 and 25. For example, if the Call Park prefix is 1, the first parked call is assigned Call Park retrieval code 101

The Park prefix must not conflict with the following:

- external code
- direct dial digit
- private access code
- Public/Private Auto DN
- Public Private DISA DN
- line pool code/destination code, or
- telephone DN

Attention: Other programmable settings can affect which numbers appearing the window during programming. Although the numbers 0 to 9 are valid Park prefix settings, some may already be assigned elsewhere by default or by programming changes. If the DN length changes, and the changed DNs conflict with the Park prefix, the setting changes to None.

The system assigns Call Park codes to calls in sequence, from the lowest to the highest, until all the codes are used. The use of different of codes ensures a call reaches the right person, especially when more than one incoming call is parked.

Attention: Model 7000 phones are supported in Europe only.

The highest call number (the Call Park prefix followed by 25) is used by model 7000 and 7100 telephones, analog telephones, or devices connected to the system using an ATA2. Analog telephones or devices cannot use the other Call Park codes.

When parking a code on an analog telephone, the call is parked on the highest park code. When retrieving a call, any phone can retrieve the call by entering the park code.

Calls are retrieved by pressing the intercom button and dialing the retrieval code. On model 7000 and analog telephones, pick up the receiver, if the call is parked by the analog phone, use <parkcode>25; otherwise, use <parkcode><parknumber>.

Attention: Analog phones can park call only at <parkcode>25.

You also need to program the park timeout. The park timeout determines when external parked calls that are not answered return to the originating telephone. You can disable Call Park by setting the Park prefix to None.

Direct dial digit

The Direct dial digit setting allows you to specify a single system-wide digit to call a direct dial telephone.

Access for user remote dialing

The remote access feature allows callers elsewhere on the private or the public network to access your BCM by dialing directly and not going through the attendant. After the remote user is in the system, they can use some of the system resources. You must enable remote access in programming before callers can use it.

Access codes, user remote dialing

BCM supports remote system access on a number of trunk types which can require the remote caller to enter a password for DISA.

The system resources, such as dialing capabilities, line pool access and feature access, that a remote user can access depends on the CoS password assigned to them. See [CoS password definition \(page 220\)](#).

Attention: Callers remotely access the BCM remote features setting by pressing * and the appropriate page code.

Private auto DN

Private network calls answered without DISA require no password to access the BCM. The type of service that applies to the call depends on the restrictions assigned to the trunk.

Public auto DN

Public network calls answered without DISA require no password to access the BCM. The type of service that applies to the call depends on the restrictions assigned to the trunk.

Private DISA DN

For private network calls answered with DISA, the system presents a stuttered dial tone to prompt a caller to enter a valid password. The Class of Service (CoS) that applies to the call is determined by this CoS password.

After a remote user accesses the BCM, they can change the existing CoS password using the DISA DN. This gives you greater flexibility when you create access privileges. For example, you may want to have a shared DN for remote access, but separate CoS passwords with different dialing out privileges for individuals.

Public DISA DN

For public network calls answered with DISA, the system presents a stuttered dial tone to prompt a caller to enter a valid password. The Class of Service (CoS) that applies to the call is determined by this CoS password.

After a remote user accesses the BCM, they can change the existing CoS using the DISA DN. This gives you greater flexibility when you create access privileges. For example, you may want to have a shared DN for remote access, but separate CoS passwords with different dialing out privileges for individuals.

Access for ingress private network calls

The Private network access code identifies this system to the private network.

The Private network access code is part of the dialing plan but not part of the numbering plan. It is used in MCDN UDP private networks. Example: If you dial 6-393-7777, the private access code is 6 but is not sent with the other dialed numbers.

Private network local access code

This number is prepended to an incoming E.164/ Local call (7 digits in North America). See [Codes for MCDN special call types \(page 41\)](#). This applies for MCDN connections only.

Private network national access code

This number is prepended to an incoming E.164/ National call (10 digits in North America). This is not directly related to the private access code. This applies for MCDN connections only.

Private network special access code

This number is prepended to an incoming E.164/ International or Private/ Special call. The incoming international call is not prepended with 011. This applies for MCDN connections only.

Access for system egress calls

This section describes access for system egress calls.

External codes, ATA and analog devices

Devices connected to the system through an ATA can have connectivity issues over BRI/PRI lines. To alleviate this, you can specify the type of device attached to the analog line.

Modem supports 3.1 kHz audio, which requires a higher quality of service on the ISDN trunks that modems and FAX machines require for reliable information transfer. If the trunks cannot provide the higher level of service, the call fails.

Telephone supports speech paths, which require less quality on the trunk; if used for FAX and/or modem, information transfer is unreliable.

Telephones use pool codes and destination codes to dial externally, because when the analog device goes off hook, it seizes internal dial tone from the system. The external access code, is either a line pool code, or destination code assigned to your system dialing plan.

Line pool access codes

Line pool access codes allow you to assign an access code for each of the basic line pools (A to O). These codes specify the line pool for making an outgoing external call. Up to three digits in length, these codes do not allow any other routing programming. The user simply dials the code in front of the dial string. The system, in turn, deletes the entire code before sending the call out over the appropriate route.

If you need a more complex routing arrangement, you need to specify routes and destination codes, which allows you more flexibility in terms of dial strings, routing schedules, and routing restrictions.

Destination codes

This number precedes a telephone number to tell the system where the call needs to be routed. An A in the destination code represents an any character designation. The A code is a wildcard.

Carrier codes

In some cases, long distance service uses the same lines as local service but is switched to a specific carrier using an access number, which is sometimes referred to as an carrier access code (CAC). Route programming can include the access number so the users do not have to dial it every time they make a long distance call.

BCM450 feature access codes

This section describes BCM450 feature access codes.

Direct dial set configuration

The Direct dial setting allows you to dial a single system-wide digit to call a specific telephone, called a direct dial telephone. The most common example of a direct dial set is a telephone for an operator, a receptionist or an attendant. You can program a maximum of five direct dial sets on the system, however, you can only specify one direct dial number for the system.

Interaction between access codes

The following list describes the interaction between different access codes:

- **External line access code:** If the DN length is changed, and the changed DNs conflict with the external line access code, the setting changes to None.
- **Direct dial telephone:** Another direct dial telephone, an extra dial telephone, can be assigned for each schedule in Services programming.
If the DN length is changed, and the changed DNs conflict with the Direct dial digit, the setting changes to None.
- **Public/Private Auto DN:** The length of the Auto DNs are the same as the Public or Private Received Number Lengths specified under Configuration > Telephony > Dialing Plan. The public/private Auto DN is cleared if the corresponding Received Number Length is changed.
- **Public/Private DISA DN:** The length of the DISA DNs are the same as the Public or Private Received number length specified under Configuration > Telephony > Dialing Plan. The public/private DISA DN is cleared if the corresponding Received number length is changed.

Attention: When configuring a private network, ensure the numbering plan does not conflict with the public telephone network. For example, in North America, using “1” as an access code in a private network, conflicts with the PSTN numbering plan for long-distance calls.

The following codes/digits must not conflict:

- park prefix

- external code
- direct dial digit
- private access code
- Public/Private Auto DN
- Public/Private DISA DN
- line pool code/destination code
- telephone DN

MCDN codes for tandem call configuration

Three special codes exist specifically for programming over PRI and VoIP trunks that are using the MCDN protocol, and which connect to a call server systems that use specific call codes for special call types, such as the Meridian 1 (M1). The purpose of the codes is to allow easier programming of the call server systems when calls are tandemed through a BCM to the local PSTN.

Calls tandeming to the public network through the private network need to retain their dialing protocol throughout the private network. This means that the BCM node receives a call from an M1 node tagged as a local call and recognizes the call intended for the public network, but also recognizes the call that needs to maintain the local call tag until it gets to the BCM node that is directly connected to the PSTN. This is accomplished by ensuring that the destination code, which starts with this access code, passes the call on using the route designated with the correct call type.

VoIP trunks for fallback feature

The following path indicates where to access setting VoIP trunks for fallback in the Element Manager:

- Element Manager: **Configuration > Resources > Telephony Resources > IP Trunks > H323 Settings tab**

Call routing configuration

Call routing allows you to define how calls are routed by your BCM system.

Call routing decides what path an outgoing call takes using the digits that are dialed. It is sometimes called Automatic Route Selection (ARS).

Call routing configuration

When you select an internal line and dial, the system checks the numbers you enter against the routing tables. If the number you dial starts with a destination code, the system uses the line pool and dials out digits specified by the route assigned to that destination code, and then dials the rest of the number that you dialed.

Routing service replaces a number of manual tasks, including:

- entering a line pool code
- dialing an access code for a long-distance carrier
- deciding which line pool to use according to the time and day
- deciding which line pool to use according to the time and day

You can set up routing to take advantage of any leased or discounted routes using information supplied by the customer. The system cannot tell what lines are cheaper to use.

For Call-by-Call service selection (PRI only), the installer defines destination codes for various call types over PRI lines (for example, Foreign Exchange, TIE Trunk, or OUTWATS). The user dials a number using the intercom button without entering any special information. For more information see [Configuration for PRI CbC limits \(page 55\)](#).

BCM450 call-by-call services

This sections describes call-by-call services.

ISDN PRI call-by-call services configuration

To program the system for Call-by-Call (CbC) Limits with a PRI interface, you must:

- provision a DTM as PRI, if one is not already configured as part of the system
- select a protocol
- program incoming call routing
- program routes that use the PRI pools, see [Call routing configuration \(page 51\)](#).

Supported protocols

The following protocols support CbC limits:

- National ISDN 2 (NI-2)
- DMS-100 custom
- DMS-250
- AT&T 4ESS custom

PRI-MCDN and IP trunks support CbC Limits to limit the number of incoming or outgoing calls only. No selection of CbC Services is provided.

3rd party switch support, CbC limits

The following table lists the service types and cross-references them with four common switches.

Table 3 Switches and service types chart

	Switches			
Service types¹	NI-2	DMS-100 (custom)	DMS-250	AT&T 4ESS
FX	FX	FX ²	N/A	N/A
Tie ³	TIE	TIE	TIE	SDN (software defined network)
INWATS	INWATS	INWATS	Eight Hundred	Toll Free MEGACOM
International NWATS	Same as INWATS	Same as INWATS	Same as INWATS	International Toll Free Service
OUTWATS	IntraLATA OUTWATS OUTWATS with bands InterLATA OUTW TS	OUTWATS	PRISM	MEGACOM
Private		DMS Private5	VNET (virtual network)	N/A
Switched Digital	N/A	N/A	N/A	ACCUNET ⁴
Nine Hundred	N/A	N/A	Nine Hundred	MultiQuest
Public	Public	Public	Public	N/A
<ul style="list-style-type: none"> N/A indicates that the protocol does not support the service. DMS-250 Sprint and UCS support incoming FX only (that is, Network-to-BCM). DMS-250 MCI does not support FX. NI-2 allows two TIE operating modes: senderized and cut-through. BCM supports only senderized mode. Rates greater than 64 kbps are not supported. Bell Canada VNET. Not all service types may be supported by a switch type. For information, contact your service provider. 				

Configuration for PRI CbC limits

Programming Call-by-Call on PRI requires these settings:

- Select Configuration > Telephony > Sets > All DNs to assign the line pool.
- Select Configuration > Telephony > Dialing Plan > Routing to assign a pool for routing, and assign the service type and service id, if required.
- Select Configuration > Telephony > Dialing Plan > Line Pools tab to specify the minimum and maximum values for the pools.

Prerequisites for PRI CbC limits

To program the system for Call-by-Call Limits with a PRI interface, you must:

- provision a DTM as PRI, if one is not already configured as part of the system
- select a protocol
- program incoming call routing
- program routes that use the PRI pools, see [Call routing configuration \(page 51\)](#).

PRI call-by-call service routing

The following table is an example of a Routing Table containing Call-by-Call programming (available in the North America market profile).

Table 4 Call-by-Call routing table example

Route Number (000-999)	Dial Out (24 digits)	Use Pool	Service Type	Service Identifier
003		BlockA	Public	xxxxx xxxxx xxx
004		BlockA	FX	
005		BlockA	TIE	
006		BlockB	OUTWATS	
007		BlockB	Private	
008		BlockB	Switched Digital	
Attention: The public DN lengths are used for all PRI calls except those whose routes use service type Private or service type TIE with DN Type specified as Private.				

PRI protocols & service/DN types

The following table lists the service/DN type choices available for PRI lines.

Table 5 PRI Service type/DN type values

PRI Protocol	Type	Values
MCDN	DN	Public, Private, Local, International, National, Special
ETSI Euro	DN	Public, Local, International, National,
ETSI QSIG	DN	Public, Private, Local, International, National,
NI	DN	Public, Private, Local, International, National,
ETSI Euro	Service	None, overlap
NI		Public, TIE, Foreign Exchange (FX), OUTWATS
DMS-100	Service	Public, Private, TIE, Foreign Exchange (FX), OUTWATS
DMSW250	Service	Public, Private, TIE, Foreign Exchange (FX), OUTWATS
4ESS	Service	TIE, OUTWATS, Switched Digital (SDS)

BCM450 destination codes

Destination codes allow you to control how the system interprets and routes dial strings from internal sources. Destination codes are similar to line pool codes except that by using routes (which attach dial strings and DN type designators to line pools) and schedules you can control what digits the user has to dial and how the system routes the call out of the system, including what numbers from the dial string get added or deleted to the route dialout.

Destination codes and how to apply

Routes determine path (line or pool) and any required access numbers.

Destination codes determine which route to take (that is, an end node uses one destination code for all other nodes in the system). If you choose to use the destination codes Normal schedule, the call always goes out over the same route. If you choose to use the other destination codes schedules, you can set up a more responsive plan, whereby calls can go out over more than one route, based on scheduled times.

Destination codes provide you with the opportunity to create a dialing plan that allows users to connect to other systems in a relatively seamless or consistent manner, regardless of the lines or routes that are being used to get there. For example, connecting through VoIP lines requires significantly different ways of dialing than dialing over T1 lines. However, you can configure destination codes, such that the user dials the same number of digits regardless of the trunks over which the calls are routed.

Destination code configuration conflicts

Destination codes must not conflict with the following:

- park prefix
- external code
- direct dial digit
- Auto DN
- DISA DN
- Private access code
- line pool codes
- telephone DN
- public target line received digits
- other destination codes

Attention: You can enter destination codes up to a maximum of 12 digits.

Attention: When configuring a private network, ensure the numbering plan does not conflict with the public telephone network. For example, in North America, using “1” as an access code in a private network, conflicts with the PSTN numbering plan for long-distance calls

Considerations for codes selection

When deciding on which digits to use to start your destination codes, consider the following:

- Ensure that the digit or digits you want to start your destination codes with do not match any of the access codes, including the line pool codes that already exist in your system. You may find that you need to delete line pool codes and create a route and destination code instead. This could occur if you want to set up fallback to a public line, for instance. If the public line is accessed by a line pool code, you would have to change access to a route so you could create a fallback schedule with the destination code used for the primary line (or lines, if you have more than one outgoing line pool that requires fallback).
- Decide how much of the common part of a dial string you want your users to have to dial, and how much you can put in the dial string.
- If you want specific dial strings to use specific routes, map these out first.

For instance, if you want users to dial between BCMs over VoIP lines, you create destination codes specific to those systems that use the VoIP line pool, using the digits with which the users are familiar. You can then create a unique destination code for the call you want to route.

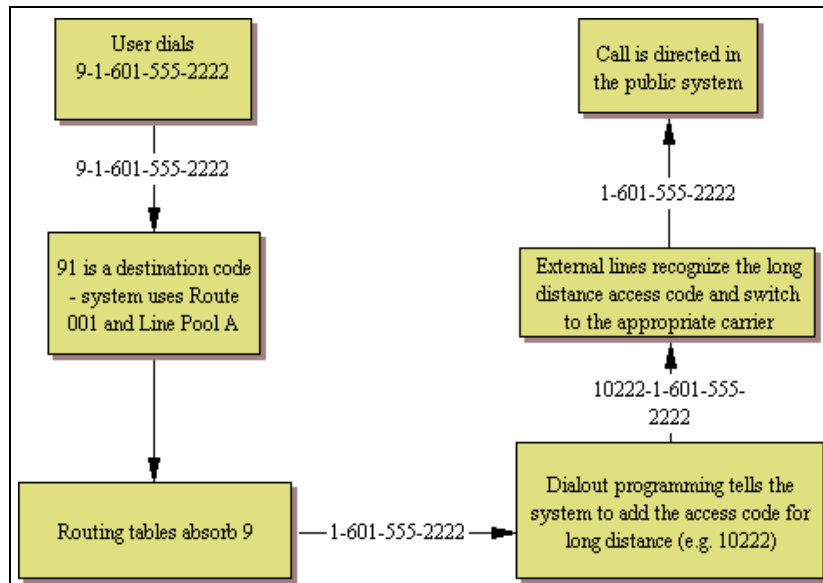
Configuration for digit absorption

The digit absorption setting (Absorbed Length) applies to a maximum of two schedules, including normal routing.

When the Absorbed Length is 0, the actual digits dialed by a caller are preserved in the dialout sequence. As you increase the absorbed length, the equivalent number of digits are removed from the beginning of the destination code.

Carrier access VS destination codes

Route programming can include the access number so the users do not have to dial it every time they make a long-distance call. The following figure shows an example of how the system interprets what the user dials into a valid outgoing call.

Figure 6 Carrier code call numbering sequence

The destination codes 9 and 91 used in the examples cannot be used together. If you need the destination code 91 to direct long-distance calls, you must create a separate set of codes that use local calling routes. These codes would be, for example, 90, 92, 93, 94, 95, 96, 97, 98 and 99. You can also use 9 A. (A represents a wildcard “Any”.)

Grouping destination codes using a wild card

If you have a number of destinations that have the same route and digit absorb length, you can group these codes under one destination code to maximize your destination code table. In this case, the start digits are the same, but the last character are the wild card, and indicates any digit between 0 and 9. However, if a conflict exists with other digits already programmed or used by other destination codes, an error message appears.

For instance, you might use the same route (555) to a number of remote sites. Each site is accessed with the same external # (dial out string), except for the last digit, which is unique to each site. The exception to this is a site with a totally different access number and line pool requirement (route 565). This example is shown in the following table.

Route	Dial out (external #)	Line pool
555	0162 237 625<unique number from 0 to 9>	Line Pool C
565	0173 133 2211	Line Pool A

If you do not use wild cards, you would need to create a separate destination code for each unique dialout, as shown in the following table.

Destination codes	Route	Absorb length	Dial out
5621	555	3	0162 237 6251
5622	555	3	0162 237 6252
5623	555	3	0162 237 6253
5624	555	3	0162 237 6254
5625	555	3	0162 237 6255
5626	555	3	0162 237 6256
5627	565	All	0173 133 2211
5628	555	3	0162 237 6258
5629	555	3	0162 237 6259

If you use the wild card character A (ANY), you can reduce the number of destination codes you require to two, as shown in the following table.

Destination codes	Route	Absorb length	Dial out
562A	555	3	0162 237 625X where X is the last digit of the destination code dialed out, from 1 to 9, but not 7
5627	565	All	0173 133 2211

Attention: To minimize the effort involved in preparing destination codes, set the digit absorption to 0. When digital absorption is set to 0, the actual digits dialed by a caller are preserved in the dial-out sequence. The need to program a dial out sequence as part of the route depends on the required dialout.

Routing schedules and alternate routes

It can be less expensive to use another long-distance carrier at a different time of day. Continuing with the example used in the previous flowchart, the lines that supply local service in normal mode are also used for long-distance service after 6 p.m. because that is when rates become competitive. For the system to do this automatically, you must build another route.

All the lines used by a route specified by a destination code are busy when a call is made, you can program other routes that the system automatically flows the calls to, or you can allow the call to overflow directly to the Normal route schedule (usually the most expensive route). However, this only takes effect if an active routing schedule is applied to the line. Overflow routing is not available in Normal mode.

You must create overflow routes for each destination code for which you want to allow overflow routing.

When a user dials, and the telephone cannot capture the preferred line (First Route), the system tries each successive defined route (Second Route, then Third Route). If none of these routes have available lines, the call reverts to the Normal mode. When the call switches from the preferred routing mode (First Route, Second Route, Third Route) to Normal mode, the telephone display flashes an “expensive route” warning. VoIP trunking uses a similar process for setting up fallback from the VoIP trunk to a PSTN line.

Attention: Overflow routing directs calls using alternate line pools. A call can be affected by different line filters when it is handled by overflow routing.

Dialing plan and routing configurations

The following paths indicate where to access the route lines and loops in Element Manager and through Telset Administration:

- Element Manager: Configuration > Telephony > Dialing Plan > Routing
- Telset interface: **CONFIG > Services > Routing Service > Routes

Configuration prerequisites for dialing plans

Complete the following prerequisites checklist before configuring the modules.

Media bay modules/VoIP trunks are installed and configured.	
Create an access code/route map to understand how the numbering works for the system.	

Destination coding in a network

Because the system checks the initial digits of a call against the routing tables, each type of internal or external call must begin with a unique pattern of digits. The following table gives a sample plan for how initial digits are assigned in a network of systems with three-digit intercom numbers.

Table 6 Destination code leading digits

Leading Digits	Use
0	Network Direct Dial
221-253	Intercom calls
4	Coordinated Dialing Plan
5	Unused
6	Unused
1	Call Park Prefix
9	All PSTN Calls
7	Unused

In the table4 is used as the initial digit for the coordinated dialing plan, but 5, or 6 can also be used for this purpose.

Attention: When programming a button to dial an external number automatically (autodial), private network calls must be programmed as external autodial numbers, even though they resemble internal extension numbers.

Routes generally define the path between the BCM system and another switch in the network, not other individual telephones on that switch.

Destination codes and code grouping

If you have a number of destinations that have the same route and digit absorb length, you can group these codes under one destination code to maximize your destination code table. In this case, the start digits are the same, but the last character is the wild card, and indicates any digit between 0 and 9. However, if a conflict exists with other digits already programmed or used by other destination codes, an error message appears.

For instance, you might use the same route (555) to a number of remote sites. Each site is accessed with the same external # (dial out string), except for the last digit, which is unique to each site. The exception to this is a site with a totally different access number and line pool requirement (route 565). This example is shown in the following table.

Table 7 Establishing routes and dialout requirements

Route	Dial Out (external #)	Line Pool
5555	0162 237 625<unique number from 0 to 9>	Line Pool C
565	0173 133 2211	Line Pool A

If you do not use wild cards, you would need to create a separate destination code for each unique dialout, as shown in the following table.

Table 8 Destination codes not using a wild card

Destination codes	Route	Absorb Length	Dial out
5621	555	3	0162 237 6251
5622	555	3	0162 237 6252
5623	555	3	0162 237 6253
5624	555	3	0162 237 6254
5625	555	3	0162 237 6255

Table 8 Destination codes not using a wild card

Destination codes	Route	Absorb Length	Dial out
5626	555	3	0162 237 6256
5627	565	All	0173 133 2211
5628	555	3	0162 237 6258
5629	555	3	0162 237 6259

If you use the wild card character A (ANY), you can reduce the number of destination codes you require to two, as shown in the following table.

Table 9 Destination codes using the ANY character

Destination codes	Route	Absorb Length	Dial out
562A	555	3	0162 237 625X where X is the last digit of the destination code dialed out, from 1 to 9, but not 7
5627	565	3	0173 133 2211

Attention: To minimize the effort involved in preparing destination codes, set the digit absorption to 0. When digital absorption is set to 0, the actual digits dialed by a caller are preserved in the dial-out sequence. The need to program a dial out sequence as part of the route depends on the required dialout.

Dialing plan—routing and destination codes

A large system usually requires a number of destination codes to ensure that calls are directed to the correct trunks, either on the private or public network.

The following paths indicate where to access destination codes in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Dialing Plan > Routing**
- Telset interface: ****CONFIG > Services > Routing Service > Routes**

The following panels allow you to

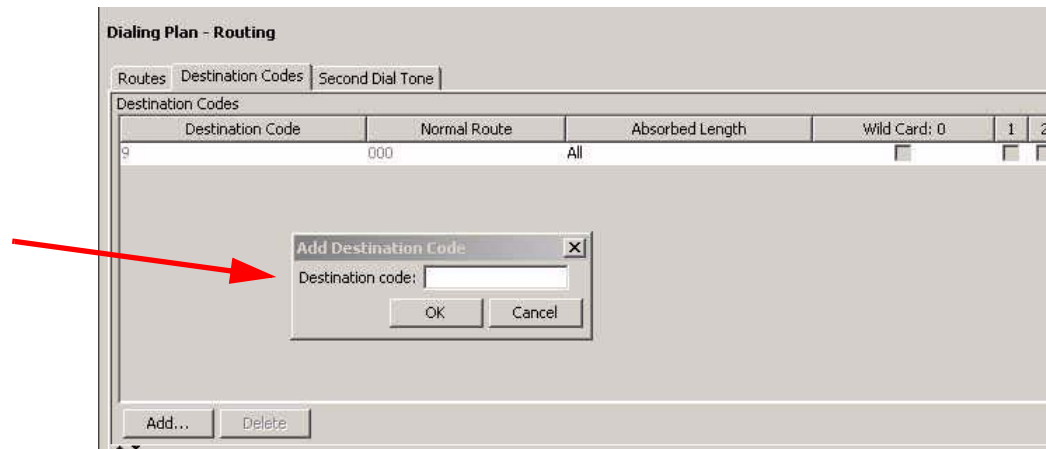
- create routes
- create destination codes for the routes, and the Normal schedule
- create alternate routing schedules

Dialing plan route configuration

The first step to setting up call routing is to define line pools into uniquely named routes. A route can be used with more than one destination code, but a line pool should only be used with one route.

The following figure illustrates the Routes tab.

Figure 7 Routes table



The following table describes the fields on the top panel.

Table 10 Route settings (Sheet 1 of 2)

Attribute	Value	Description
Route	<001-999>	This number is unique to each route
External Number	<a maximum of 24 digits>	<p>Enter the external or dial-out number for the route you want the assigned telephone to use. The external number is a digit or group of digits that get inserted in front of your dialed digits. If all the required numbers are defined in the destination code/dial string, this box can be left empty.</p> <p>Optional entries in the dial string:</p> <p>P = 1.5 second pause (counts as one digit in the dialing string) (F78 telset)</p> <p>DT = wait for dial tone (counts as two digits in the dialing string)</p> <p>(F804 telset)</p>
Use Pool	Pool A to Pool O or BlocA to BlocF	<p>Select a line pool for the route.</p> <p>The Bloc pools only display if you have PRI or VoIP trunks.</p>
DN Type	Public Private Local (Subscriber) National Special (International)	<p>This setting tells the system what type of line protocol the route uses to process the dial string. Refer to PRI route types (page 71)</p> <p>MCDN private networks: Local, National, and Special are special designators used to route calls from Meridian 1 systems, through BCM systems, out to the public network. Select Configuration > Telephony > Dialing plan > Private Networks tab to define the codes for these settings.</p> <p>When the BCM receives outgoing calls from the Meridian 1, it recognizes the call type and appends the appropriate access code to the Meridian dial string.</p> <p>This code then matches to a route that uses the same DN type, passing the call along, either to another node (the route would have the same DN type) or to the public network (the route would have a Public DN type), depending on the routing information.</p>

Table 10 Route settings (Sheet 1 of 2)

Attribute	Value	Description
Service Type	Public Private TIE Foreign exchange (FX) OUTWATS Switched Digital (SDS) None Overlap	This setting tells the system what type of line protocol the route uses to process the dial string. These protocols are used for lines connected to DMS-100, DMS-250 and 4ESS switches. Refer to PRI route types (page 71)
Service ID	<digits>	If you choose a service, type in the identification number for the service.

Table 11 Route settings (Sheet 2 of 2)

Attribute	value	description
Note	Outgoing call display: If you have the trunks set up to send called number information, and the DN type is set to anything, except Private, the system sends the Public OLI number you specified under line programming. If the DN type is set to Private, the system sends the Private OLI number.	
Actions:		
Add	<ul style="list-style-type: none">Under the routes table, click Add.Enter a route number in the dialog boxClick OK to save the new route.	
Delete	<ul style="list-style-type: none">On the routes table, select the route you want to delete.In the Routes pane, click Delete.Click OK.	
Modifying routes:	<p>Attention: Modifying some route settings may result in dropped calls. Ensure that you modify the destination codes Absorbed Length setting, if required, if you add or change the External Number entry.</p> <p>Changing the Use Pool or DN Types/Service Types values results in dropped calls the lines in the line pool do not support the DN/Service Type selected.</p> <ul style="list-style-type: none">On the routes table, select the route you want to change.Click the field you want to change for that route and enter the new valuePress Tab on your keyboard to save the change	

PRI route types

The following table lists the service/DN type choices available for PRI lines

Table 12 PRI Service type/DN type values

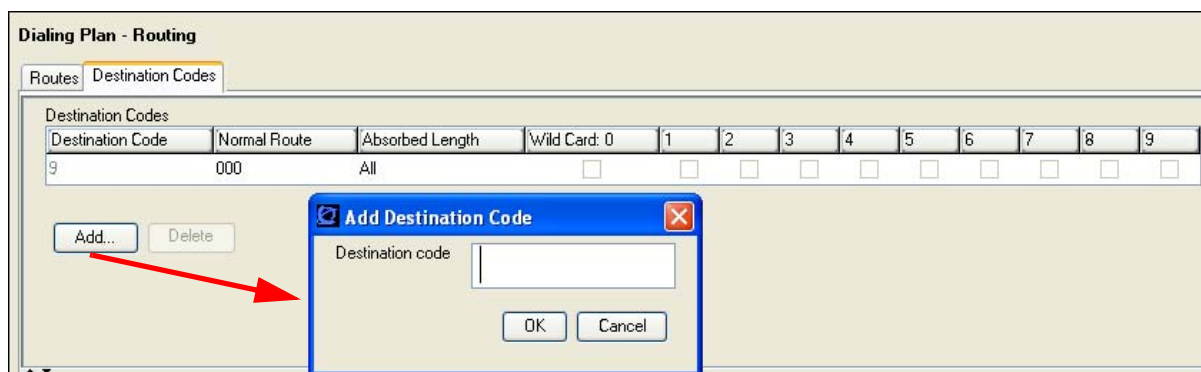
PRI Protocol	Type	Values
MCDN	DN	Public, Private, Local, International, National, Special
ETSI Euro	DN	Public, Local, International, National
ETSI QSIG	DN	Public, Private, Local, International, National
NI	DN	Public, Private, Local, International, National
ETSI Euro	Service	None, Overlap
NI	Service	Public, TIE, Foreign Exchange (FX), OUTWATS
DMS-100	Service	Public, Private, TIE, Foreign Exchange (FX), OUTWATS

Dialing plan destination code configuration

Once you have the routes configured, set up the dialing plan destination codes that allow users to access the routes. You can use a route for more than one destination code, as you may require different codes for the same route to define restrictions or special call designators. To access the dialing plan routing tab, click Configuration> Telephony> Dialing Plan> Routing.

The following figure illustrates the Destination codes panel.

Figure 8 Destination codes table panel



The following table describes the fields on the destination codes frame.

Table 13 Destination codes table

Attribute	Value	Description
Destination Code	<max.12 digits>	This number precedes a telephone number to tell the system where the call needs to be routed. An A in the destination code represents an any character designation. The A code is a wildcard.
Normal Route	<configured route #>	This is the route that the system uses when the destination code is added to the dial string.
Absorbed Length	All, None, 1-X	This indicates how much of the destination code gets removed before the system sends the dial string to the network.
Wild Card 0-9	Included, Excluded, Unavailable	If you enter the wild card character A at the end of a destination code, then the following applies: Included: This number can be dialed as part of the destination code Excluded: This number is not accepted as part of a destination code string because it is already used in the system. Unavailable: This number is already defined in another destination code and cannot be used
Add	<ul style="list-style-type: none">• Under the Destination Codes table, click Add.• Enter the new destination code.• Click OK to save the route settings.• On the Destination Codes table, select the fields beside the route you just created, and modify them, as required.• Test the route.	
Delete	<ul style="list-style-type: none">• On the Destination Codes table, select the destination code you want to delete.• In the Destination Codes pane, click Delete.• Click OK.	

The destination codes must not conflict with the following:

- park prefix
- external code
- direct dial digit
- Auto DN
- DISA DN

- Private access code
- line pool codes
- telephone DN
- public target line received digits
- other routing codes

Dialing plan alternate routing schedules

When you select a route on the Destination Codes panel, the alternate schedules for that route appear in a separate table. You only need to fill out this panel if your system is using routing schedules.

Note that in these schedules you can configure three routes. The second route acts as fallback route for the first route if it is unavailable. If the second route is also unavailable, the system tries the third route. The dialing sequence for these routes needs to be the same from the user perspective, as fallback occurs automatically and is not controlled by the user. If all three routes fail, the default normal route is used.

The following figure illustrates the Alternate Routes panel.

Figure 9 Alternate routing schedules

Alternate Routes for Destination Code: 9

Alternate Routes						
Schedule	First Route	Absorbed Length	Second Route	Absorbed Length	Third Route	Absorbed Length
Night		All		All		All
Evening		All		All		All
Lunch		All		All		All
Sched 4		All		All		All
Sched 5		All		All		All
Sched 6		All		All		All

The following table describes the fields on the Destination codes frame.

Table 14 Destination codes schedules

Attribute	Value	Description
Schedule	Defaults: Night, Evening, Lunch, Weekend, Sched. 5, Sched. 6	If you use a different carrier at different times of the day or week, you can set the destination code to use that route and provide two more backup routes. The user does not experience any difference in dialing sequence
First Route	<configured route #>	This is the route that the system uses, during the indicated schedule, when the destination code is added to the dial string.
Absorbed Length	All, None, 1-X	This indicates how much of the destination code gets removed before the system sends the dial string to the network.
Second Route	<configured route #>	This is the route the system uses if the first route is unavailable
Absorbed Length	All, None, 1-X	This indicates how much of the destination code gets removed before the system sends the dial string to the network.
Third Route	<configured route #>	This is the route the system uses if the first and second route are unavailable.
Absorbed length	All, None, 1-X	This indicates how much of the destination code gets removed before the system sends the dial string to the network.

Second dial tone for outgoing PRI

This feature provides dial tone for outgoing calls on any PRI line, based on the digits dialed. Digits dialed must match an entry in the second dial tone table to enable a second dial tone. Dial tone occurs on the line until another digit is dialed, a timeout occurs, or the user hangs up.

Up to 10 separate entries can be stored in the second dial tone table. The maximum digit length for each entry is four. Each entry must be unique and cannot conflict with:

- Internal DNs
- Hunt Group DNs
- DISA DNs
- Auto DNs
- Target Line DNs

Attention: Entries can match destination or access codes for outgoing lines.

The following paths indicate where to configure the Second Dial Tone in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Dialing Plan > Routing > Second Dial Tone**
- Telset interface: ****CONFIG > Services > Routing Service > 2nd Dial Tone**

Figure 10 Second Dial tone

The screenshot shows a web-based configuration interface titled "Dialing Plan - Routing". It has three tabs: "Routes", "Destination Codes", and "Second Dial Tone", with the last one being active. Under the "Second Dial Tone" tab, there is a section labeled "SDT Prefix List". Inside this section, there is a text input field containing "SDT Prefixes". Below the input field is a list box containing the numbers 32, 33, 34, and 41. At the bottom of the list box area, there are two buttons: "Add..." and "Delete".

Table 15 Second Dial tone

Attribute	value	Description
SDT Prefix list		
SDT Prefixes		Enter the digits to match to trigger a second dial tone.
Actions		
Add	Button	Add SDT Prefix to list
Delete	Button	

Attention: Second dial tone is not provided on outgoing lines for remote access users and for ISDN terminal users when the Call Transfer feature is activated.

Attention: A second dial tone is not provided if an SDT prefix is entered as an External Autodial (Feature *1).

Dialing plan configuration for public network

This section gives an overview of dialing plan configuration for public network. The panel described in the following information defines the number planning required for calls exiting the system to the public telephone network.

Public dialing plan settings

The Dialing Plan - Public Network panel displays the fields that determine dialing information specific to dialing in or out to a public network from the host system. To access the Public Network panel, click Configuration > Telephony > Dialing Plan > Private Network.

This panel includes information about

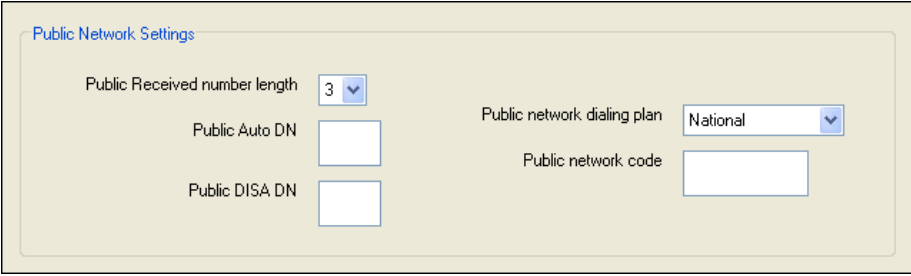
- [Public network settings \(page 77\)](#)
- [Public network DN lengths \(page 80\)](#)
- [Carrier code settings \(page 82\)](#)

Public network settings

This following describes system settings that allow the system to determine if an incoming call is meant for the local system. These settings determine how many digits the system needs to receive before sending the dial string over the trunk interface.

The following figure illustrates the Public Network Settings panel.

Figure 11 Public Network Settings pane



The image shows a configuration pane titled "Public Network Settings". It contains five fields arranged in two columns. The left column has three fields: "Public Received number length" with a dropdown menu showing "3", "Public Auto DN" with an empty text box, and "Public DISA DN" with an empty text box. The right column has two fields: "Public network dialing plan" with a dropdown menu showing "National", and "Public network code" with an empty text box.

Public Network Settings	
Public Received number length	3
Public Auto DN	
Public DISA DN	
Public network dialing plan	National
Public network code	

The following table describes each field in the Public Network Settings box.

Table 16 Private and Public received numbers

Attribute	Value	Description
Public Received number length (max)	<2-12>	The maximum number of digits (2, 3, 4, 5, 6, 7) that the system uses to determine if an incoming call tagged as public fits the system public DN numbering. Default: DID template, same as DN length; PBX template: 3
Public auto DN	<DN digits to be received from the auto-answer trunk>	Public network calls answered without DISA require no password to access the BCM. The type of service that applies to the call depends on the restrictions assigned to the trunk.
Public DISA DN	<DISA DN digit to be received from the auto-answer trunk>	For public network calls answered with DISA, the system presents a stuttered dial tone to prompt a caller to enter a valid password. The Class of Service (CoS) that applies to the call is determined by this CoS password. After a remote user accesses the BCM, they can change the existing CoS using the DISA DN. This gives you greater flexibility when you create access privileges. For example, you may want to have a shared DN for remote access, but separate CoS passwords with different dialing out privileges for individuals.
Public network dialing plan	National Local Public	Local dialing plan defines a seven-digit numbering scheme. National dialing plans define an extended number scheme. North America is set to 10 digits. However, systems in other countries may have a variable length Public dialing plan is variable length
Public network code	<1-7 digits>	This number concatenates with the Public OLI, which, by default, is the DN of the device. In systems running the North American profile, if the Public OLI contains the public network code, that entry overrides any entry in this field.

Public network DN lengths

The Public network DN length tells the system how long dialing strings are when entering the network. For example, if you dial 18005551212 the public network DN length for 1, which is 11, tells the system to wait until 11 digits are entered before processing the call. To access the Public Network DN lengths tab, click Configuration > Telephony > Dialing Plan > Public Network.

Attention: If the values for Public Network DN length are set too short, digits are stripped from the dialing string. Conversely, if the values are set too large, the dialing takes longer to process.

Figure 12 Public Network DN Lengths/Carrier Codes panels

DN Prefix	DN Length
0	11
00	12
01	17
1	11
011	18
411	3
911	3
Default	7

Code Prefix	ID Length
10	3
101	4

The following table describes each field on this panel.

Table 17 Public network DN values

Attribute	Value	Description
DN Prefix	<xxxx>	This is the number that must precede a dial string exiting the system to the public network. Each prefix defines a specific destination or type of call.
DN Length	<1-25>	This number indicates how many numbers, starting from the front of the dial string, the system waits before sending to the public network

Public network DN lengths table

In the public Network DN lengths table:

- You can define up to 30 entries.
- Each entry consists of a DN prefix string (1 to 10 digits) and a length value (two digits, 1 - 25).
- Several entries are predefined in the North America profile. These defaults can handle most regions in North America without the need for additional programming. If required, you can remove or modify these entries.
- The table always contains one default entry. You cannot remove this entry. You can only modify the length parameter associated with this entry. The default entry specifies the length of any dialing string that does not match one of the other table entries.

Outgoing public calls routing

Outgoing public calls from within the system typically have the routes set to Public. The NPI/TON gets sent as Unknown/Unknown. The public called number length is based on the Public DN lengths table in the Public networks dialing plan

MCDN trunks also allow public call types when tandeming calls from another system on the private network. Some of these systems use specific call types that the BCM needs to recognize to pass on correctly.

Type of call	NPI/TON	BCM prepend access code	BCM monitor display
Local	E164/Local	Local access code (9)	E.164/Subscriber
National	E164/National	National access code (X1)	E.164/National
Special calls (international, 911, etc.)	Private/Special	Special access code (9)	

Carrier code settings

The Carrier Codes table allows you to enter a maximum of five carrier code prefixes.

- You can define up to five carrier codes.
- Entries may be predefined for a specific country profile, but you can remove these defaults.
- Each entry consists of an equal access identifier code prefix (one to six digits) and a carrier identification code length (one digit, 1 to 9).
- Each entry is identified by the prefix digits themselves.

The following table describes each field on this panel.

Table 18 Carrier Code values

Attribute	Value	Description
Code Prefix	<one to six digits> (Read-only)	This value defines the prefix that is used to access the carrier code.
ID Length	1, 2, 3, 4, 5, 6, 7, 8, or 9	This value describes the carrier ID length

Dialing plan configuration for private networks

This section gives an overview of the dialing plan configuration for private networks. The panels described in the following information define various system settings that affect or that are affected by number planning for private networks.

Private network dialing plan configuration

The boxes on the Private Network Settings panel have fields that apply specifically to private network configurations. Network configurations can be set up between BCM systems, between BCM systems and other call servers such as the Business Communications Manager, Meridian 1, or Succession 1000. To access the Private Network Settings panel, click Configuration > Telephony > Dialing Plan > Private Network.

Some of the settings on this panel also depend on the market profile of the system.

- [Private network settings \(page 83\)](#)
- [Private MCDN network configuration \(page 86\)](#)
- [ETSI-specific network features \(page 88\)](#)

Private network settings

The settings on the Private Network Settings panel describe the numbering that the system uses to assess an incoming call to determine if the call is destined for your system or needs to be routed elsewhere on the private or public network. This panel is illustrated

Attention: When configuring a private network, ensure the numbering plan does not conflict with the public telephone network. For example, in North America, using “1” as an access code in a private network, conflicts with the PSTN numbering plan for long distance calls.

Figure 13 Private Network Settings panel

The screenshot shows a configuration window titled "Dialing Plan - Private Network". Inside, there is a section titled "Private Network Settings". This section contains two columns of settings. The left column includes "Private Received number length" (a dropdown menu set to 3), "Private Auto DN" (an empty text box), "Private DISA DN" (an empty text box), and "Private access code" (an empty text box). The right column includes "Private network type" (a dropdown menu set to CDP), "Private network ID" (a dropdown menu set to 1), "Location code" (an empty text box), and "Private DN length" (a dropdown menu set to 3).

Field	Value
Private Received number length	3
Private Auto DN	
Private DISA DN	
Private access code	
Private network type	CDP
Private network ID	1
Location code	
Private DN length	3

The following table describes each field on this panel.

Table 19 Private Network Settings

Attribute	Value	Description
Private Network Settings		
Private Received number length	2,3,4,5,6,7	The number of digits of an incoming dial string that the system uses to determine if a call tagged as Private fits the system private DN numbering. Default: DID template, same as DN length.
* Private Auto DN	<Digits to be received from a private auto-answer trunk>	Private network calls answered without DISA require no password to access the BCM. The type of service that applies to the call depends on the restrictions assigned to the trunk
* Private DISA DN	<DISA DN digits to be received from the auto-answer trunk>	For private network calls answered with DISA, the system presents a stuttered dial tone to prompt a caller to enter a valid password. The Class of Service (CoS) that applies to the call is determined by this CoS password. After a remote user accesses the BCM, they can change the existing CoS password using the DISA DN. This gives you greater flexibility when you create access privileges. For example, you may want to have a shared DN for remote access, but separate CoS passwords with different dialing out privileges for individuals.
Private access code	<systemcode> MCDN: coordinate with Dest codes	This code identifies this system to the private network The Private access code is part of the dialing plan but not part of the numbering plan. It is used in MCDN UDP private networks Example: If you dial 6-393-7777, the private access code is 6 but is not sent with the other dialed numbers.
Private network type	CDP, UDP, None	You can specify if your Private network uses a coordinated dialing plan (CDP) or a universal dialing plan (UDP). If you choose None, the private networking supplementary services are not available

Table 19 Private Network Settings

Attribute	Value	Description
Location code	<up to seven digits>	This code identifies this particular system for calls within the network for a UDP dialing plan. This number must be unique Attention: The system uses the Private Access Code length, plus the Location code length, plus the DN length to determine the DN length required to determine that a call is a private network call.
*Private DN length	3-14	The Private DN length parameter specifies the length of a dial string that the system uses to determine that the call is a private network call, when the route uses DN Type: Private.
* CDP and UDP private DN lengths are determined this way: CDP: the system uses the private received digit length UDP: the system combines the private access code length + location code length + private received digit length. When a call comes in, the system recognizes the leading digits as a private call and removes (truncates) them, leaving the private received digits, which is recognized as the private DN length.		

Private MCDN network configuration

If your system is part of a private network using the MCDN protocol, you may need to configure these special dialing access codes and network settings.

The following figure illustrates the MCDN panel.

Figure 14 MCDN network values

The image shows a configuration window titled "MCDN". Inside the window, there are six settings:

- Local access code:** A text input field.
- National access code:** A text input field.
- Special access code:** A text input field.
- Network ICCL:** A checkbox, currently unchecked.
- TRD:** A checkbox, currently checked.
- TAT:** A checkbox, currently unchecked.

The following table describes the values for these fields.

Table 20 Private network values

Attribute	Value	Description
<p>Private networking also provides access to tandem calling and toll bypass functionality to users calling into the system.</p> <p>For example, a PSTN user in Toronto could call a PSTN user in Ottawa and have the call routed over the private network connection from the Toronto office to the Ottawa office and then out to the PSTN from the Ottawa office. This bypasses any long distance toll charges.</p> <p>BCM to BCM to PSTN: Calls are routed as private over the private network and then flagged as public to go out to the end node PSTN.</p> <p>Meridian to BCM to PSTN: Special call codes from the Meridian (Local, National, and Special access codes) need to be recognized by the BCM and correctly passed to the local PSTN.</p>		
Local access code	<code to access local PSTN>	<p>MCDN connections only.</p> <p>This number is prepended to an incoming E.164/Local call (7 digits in North America).</p>
National access code	<private access code + 1>	<p>MCDN connections only</p> <p>This number is prepended to an incoming E.164/National call (10 digits in North America). This is not directly related to the private access code</p>
Special access code	<code to access local PSTN>	<p>MCDN connections only</p> <p>This number is prepended to an incoming E.164/International or Private/Special call. The incoming international call is not prepended with 011.</p>
<p>Incoming and tandem calls.</p> <p>See Private network—Destination codes (page 145)</p>		
Network ICCL	<check box>	ISDN Call Connection Limitation is part of the call initiation request. This feature acts as a check at transit PBX points to prevent misconfigured routes or calls with errors from blocking channels.
TRO	<check box>	Trunk Route Optimization occurs during the call setup. This feature finds the most direct route through the network to send a call between nodes
TAT	<check box>	Trunk anti-tromboning works during an active call to find the optimum routing.
These features require compatible programming on the remote system		

VoIP-specific private network DP config

The features contained in the VoIP subpanel are required for installations where the remote call server requires bandwidth management to handle calls

The following figure illustrates the VoIP panel.

Figure 15 VoIP special dialing plan settings

VoIP

Virtual Private Network ID 0

Zone ID 0

Use the following table to determine the settings you want to define network services feature availability.

Table 21 VoIP special dialing plan values

Attribute	Value	Description
Virtual Private Network ID	<digits>	Default:0 This is the VPN ID for a remote system, such as Succession 1000/M. In some applications, such as for the Survivable Remote Gateway (SRG) acting as a Branch Office, this ID is required to ensure that Bandwidth Management is handled correctly for calls coming into the Succession 1000/M from your system. See “VPN overview” on page 555 for more information on VPN.
Zone ID	<digits>	Default:0 A remote system, such as Succession 1000/M, may configure your system into a separate zone to accommodate specific dialing requirements, such as for an SRG system acting as a Branch Office to a Succession 1000/M system. The system administrator of the Succession 1000/M system provides the Zone ID. Enter that number here and include it in any destination codes directed to, or through, that system so that the remote system can correctly direct incoming calls.

ETSI-specific network features

The features contained in the ETSI subpanel are service provider-based network services available for some PRI-ETSI lines. This subpanel is illustrated in the following Figure.

Figure 16 ETSI private network settings

ETSI

Network Diversion ☐

MCID ☐

Use the following table to determine the settings you want to define network services feature availability.

Table 22 ETSI, MCDN, and VoIP trunk private network settings fields

Attribute	Value	Description
Network Diversion	<check box>	Allows you to choose if you want to allow calls to be redirected to an outside network.
MCID	<check box>	<p>If you select this check box, the called party can use FEATURE 897 to request the service provider network to record the identity of an incoming call. Including:</p> <ul style="list-style-type: none"> called party number calling party number local time and date of the activity calling party sub-address, if provided by the calling user
	MCID note:	<p>The feature code must be entered within 25 seconds of the caller hanging up (a 25-second busy tone occurs). If the called party hangs up first, there is no opportunity to use the feature.</p> <p>Attention: The call identification comes from your service provider, not the local system. You must have the service activated by the CO before the feature is active for the user, regardless of the setting in this field.</p>

Outgoing private calls routing

When you set up routing for private calls, the route is set to Private.

Outgoing private calls routing

How the system identifies the call depends on the type of trunk chosen for the route. Refer to the following table.

Dialing plan setting	NPI/TON	Private called number length based on
MCDN trunks send private calls in this way:		
None	Private/Subscriber	Private DN length (set on Private Network panel)
UDP	Private/UDP	private access code + home location code (LOC) + private received digits
CDP	Private/CDP	private received digit
DMS-100/DMS-250/ETSI-QSIG trunks send private calls in this way:		

Dialing plan setting	NPI/TON	Private called number length based on
None	Private/Subscriber	Private DN length (set on Private Network panel)
UDP	Private/Subscriber	private access code + home location code(LOC) + private received digits
CDP	Private/Subscriber	private received digit

Dialing plan configuration for line pools and access codes

This section gives an overview of dialing plan configuration for line pools and access codes.

Line pools and access codes for dialing plans

The panel in the top frame displays settings that are configured on other panels. The only setting you can modify on this table is the access code number. The following figure illustrates this panel. To access the Line Pools table, click Configuration > Telephony > Dialing Plan > Line Pools.

Figure 17 Dialing Plan—Line Pools table

Pool	Access Code
A	
B	
C	
D	
E	
F	
G	
H	
I	
J	
K	
L	
M	
N	
O	
BlocA	N/A
BlocB	N/A
BlocC	N/A
BlocD	N/A
BlocE	N/A
BlocF	N/A

The following table describes the fields on the top frame.

Table 23 Line Pools table fields

Attribute	Value	Description
Pool	<read-only>	These are the available line pools. Program only the ones for which you have actually assigned lines. Line pools are configured on the Lines panel
Access Code	xxx	Use access codes if you are not using destination codes on the system. These codes serve the same purpose, without the ability to define dialing sequences and multiple codes per route.

Attention: You cannot assign Bloc line pools with a line pool access code. You must define Bloc line pools under routing, and create destination codes for the routes.

Potential line pool number conflicts

The line pool number must not conflict with the following:

- park prefix
- external code
- direct dial digits
- private access code
- Public/Private Auto DN
- Public/Private DISA DN
- Telephone DN

If the line pool code and the external code start with the same digit, the line pool code programming supersedes the external code.

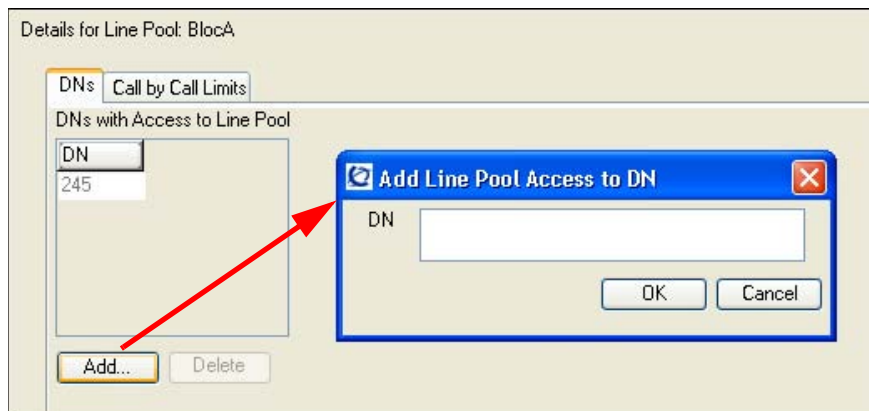
Line pools and DN

The DN tab shows you which DNs have this line pool assigned. To access the DN tab, click Configuration > Telephony > Dialing Plan > DNs.

Programming note: A line pool must be assigned to a telephone before the user can use the line pool access code (or destination code) to make a call.

The following figure illustrates the DNs tab.

Figure 18 DN access to line pools



The following table describes the fields on the DNs tab.

Table 24 Line Pools: DN access to line pools fields

Attribute	Value	Description
DNs	<read-only>	The telephones assigned to the line pool.
Actions:		
Add	<ul style="list-style-type: none"> In the Line Pools table, select the line pool you want to modify. Under the DNs tab table, click Add. Enter the DN you want to assign to the line pool. Click OK to save. 	
Delete	<ul style="list-style-type: none"> In the Line Pools table, select the line pool you want to modify In the DNs tab table, select the DN you want to delete. Under the DNs tab table, click Delete. Click OK. 	

Line pool call-by-call limits (PRI)

For PRI lines that provide Call-by-Call services, Bloc line pools have an additional configuration that allows you to configure service type limitations. For information on PRI protocols, refer to the table.

The following figure illustrates the Call-by-Call Limits tab.

Figure 19 Line Pools: Call-by-Call Limits fields

Service Type	Minimum Incoming	Maximum Incoming	Minimum Outgoing	Maximum Outgoing
Public	0	23	0	23

The following table describes the fields on the Lines tab.

Table 25 Line Pools: Call-by-Call limits fields

Attribute	Value	Description
Service Type	<read-only>	This is the type of CbC service provided on the PRI trunks in the line pool.
Minimum Incoming	Default: 2	Attention: The total of the minimum values for incoming or outgoing PRI services cannot exceed the total number of lines in the Blocpool. The maximum value for an incoming or outgoing PRI service cannot exceed the total number of lines in the Bloc pool.
Maximum incoming	Default: 23	
Minimum Outgoing	Default:4	
Maximum Outgoing	Default:23	

Private networking—basic parameters

The following provides an overview of the values in the system that affect private networking, including:

- [Private networking protocols \(page 97\)](#)
- [Keycode requirements \(page 99\)](#)
- [Scope of remote access to networking \(page 98\)](#)
- [Programming effects on private networks \(page 98\)](#)
- [Types of private networks \(page 97\)](#)

Types of private networks

There are several ways you can create private networks. Configuration can be based on such things as cost of trunks, proximity of network nodes, size of the private network, and business requirements for communications.

VoIP-based networking also requires an understanding of IP features such as codecs, jitter buffers, Quality of Service (QoS) function, a silence suppression.

The services provided within networks is based on the type of trunks and the protocols assigned to the trunks. All trunks within the network should be running the same protocols, to provide a consistent look and feel to the users.

These are the main types of private networking, listed from the simplest to the more complex PRI/ ETSI and VoIP routing using MCDN protocols:

- [Private network—Destination codes \(page 145\)](#)
- [Private networking—PRI call-by-call services \(page 149\)](#)
- [Private networking—PRI and VoIP tandem network \(page 125\)](#)
- [Private networking—MCDN over PRI and VoIP \(page 111\)](#)
- [Private networking—DPNSS network services \(UK\) \(page 135\)](#)

Private networking protocols

The BCM supports the following protocols for private networking:

- PRI: ETSI QSIG, MCDN, DPNSS

- BRI: ETSI QSIG
- T1: E&M
- VoIP: MCDN

BCM systems can be networked together using TIE lines or E&M connections. Larger networks, or networks that are geographically spread out, can be chained together through faster PRI SL-1 connections or with voice over IP (VoIP) trunk lines. SL-1 lines and VoIP trunks also offer the opportunity to use the MCDN protocol, which provides enhanced trunking features and end-to-end user identification. If a Meridian 1 is part of the MCDN network, the network can also provide centralized voice mail and auto attendant off the Meridian.

Attention: MCDN networking requires all nodes on the network to use a common Universal Dialing plan (UDP) or a Coordinated Dialing Plan (CDP).

Scope of remote access to networking

Authorized users can access TIE lines, central office lines, and BCM features from outside the system. Remote users accessing a private network configured over a large geographical area, can potentially also place long-distance calls through the network and avoid toll charges.

Attention: You cannot program a Private DISA DN or Private Auto DN to a VoIP trunk, as they act as auto-answer trunks from one private network to the next. However, you can configure VoIP line pools with remote access packages so that callers can access telephones or the local PSTN on remote nodes on a tandemed network that use VoIP trunks between systems.

Programming effects on private networks

Besides the line programming, these links connect to other programming that affects or is affected by private networks.

- [Dialing plan system-level settings \(page 101\)](#)
- [Line configuration overview \(page 15\)](#)
- [Target line configuration \(page 15\)](#)
- [Dialing plan and routing configurations \(page 63\)](#)
- [Restriction filters \(page 213\)](#)
- [Remote access packages definitions \(page 219\)](#)
- [Calling line identification \(page 29\)](#)

Keycode requirements

Keycodes are required to activate the protocols that are used to create private networking, including:

- IP trunks, if you want additional IP trunks
- an MCDN, QSIG, and DPNSS keycode to use the MCDN protocol between systems

You must purchase and install these keycodes before you can create any of the networks described in this chapter. Consult with your Nortel distributor to ensure you order the correct keycodes for the type of network you want to create.

Dialing plan system-level settings

This section gives an overview of system-level settings of Dialing plan.

Dialing plan global settings

The fields on the Dialing Plan - General panel allow you to set some general system dialing features. To access the Dialing Plan - General panel, click Configuration > Telephony > Dialing Plans > General.

The following figure illustrates the Dialing Plan - General panel.

Figure 20 Dialing Plan - General settings and Direct Dial devices

Dialing Plan - General

Global Settings

DN length (intercom)

Dialing timeout

Change DN

Access Codes

Park prefix

External code

Direct Dial

Direct Dial digit

Direct Dial Sets

Set	Type	Internal DN	External No.	Facility
1	Internal	221	N/A	N/A
2	None	N/A	N/A	N/A
3	None	N/A	N/A	N/A
4	None	N/A	N/A	N/A
5	None	N/A	N/A	N/A

System-level access codes

Refer to the following table for System-level access codes.

Attribute	Value	Description
Access codes		
Park prefix	None <one-digit number>	<p>The Park prefix is the first digit of the call park retrieval code that a user enters to retrieve a parked call. If the Park prefix is set to None, calls cannot be parked.</p> <p>Refer to Call park codes at system level (page 105) before choosing a number.</p> <p>Attention: If this field is set to None, the system-wide call appearance (SWCA) feature does not work.</p>
External code	None <one-digit number>	<p>The External code setting allows you to assign the external line access code for 7100 and 7000 digital phones and analog telephones attached to ATA 2s or to analog modules to access external lines. Note: Model 7000 phones are supported in Europe only. When the caller picks up the handset, the system tone sounds. The caller then enters this number to access an external line. Note: This number is overridden by line pool or starting with the same digit(s).</p> <p>Refer to Access codes at system level (page 104) before choosing a number.</p>

List of direct dial sets

Refer to the following table for the list of direct dial sets

Attribute	Value	Description
Direct dial sets		
Set	<1-5>	This tags the telephone to the system.
Type	Internal External None	This is the type of number for the direct-dial set.
Internal DN	DN	The DN number of the telephone to be designated as the direct dial set. (Internal sets).
External No.	<external dial string>	The actual phone number, including destination codes, of the direct dial set (External sets).

DN length configuration constraints

Certain DN length configuration constraints are as follows:



WARNING

Risk of service loss

Do not change DN length immediately after a system startup.

You must wait until the system is operational with two solid green status LEDs.



WARNING

Risk of service loss

Increasing the DN length affects other areas of the system:

If the DN length change creates a conflict with the Park prefix, external line access code, direct-dial digit, or any line pool access code, the setting for the prefix or code changes to None, and the corresponding feature is disabled.

Optional applications affected by DN length changes:

Voice mail and Contact Center applications are reset if you change the DN length after these services are installed.

Received number length in system level configuration

If you change the received number length for your system, the Public number entry for the target lines clears if the new received # length is less than the number entered in this field.

If the new received number length has more digits than the number entered in the target lines Public Number field, the entry remains, but does not update to the new DN length.

A private OLI is automatically assigned to the DNs if the DN length and the Received number length are the same. If either changes so that they are not the same, the private OLI field is cleared or not assigned (PBX template).

Access codes at system level

Here are some pointers to assist you in planning the access codes for your system.

The following values must not conflict:

- Park prefix
- external code
- direct dial digit

- Private access code
- Public/Private Auto DN
- Public/Private DISA DN
- line pool code/destination code
- telephone DN

Attention: If the line pool code and the external code start with the same digit, the line pool code programming supersedes the external code.

Call park codes at system level

When you park a call (FEATURE 74), the system assigns one of 25 codes for the retrieval of the call. You can then press the Page display key to announce the code that appears on the display.

These three-digit codes include the Call Park prefix, which can be any digit from 1 to 9, and a two-digit call number between 01 and 25. For example, if the Call Park prefix is 1, the first parked call is assigned Call Park retrieval code 101.

Attention: The park prefix must not conflict with the following:

- park prefix
- external code
- Direct dial digit
- Private access code
- Public/Private Auto DN
- Public/Private DISA DN
- line pool code/destination code
- telephone DN

Attention: Other programmable settings may affect what numbers appear in the window during programming. Although the numbers 0 to 9 are valid Park prefix settings, some may already be assigned elsewhere by default or by programming changes.

Attention: If the DN length changes, and the changed DNs conflict with the Park prefix, the setting changes to None.

The system assigns Call Park codes to calls in sequence, from the lowest to the highest, until all the codes are used. A round-robin method means the use of different codes ensures a call reaches the right person, especially when more than one incoming call is parked.

The highest call number (the Call Park prefix followed by 25) is used by model 7000 and 7100 telephones, analog telephones, or devices connected to the system using an ATA2. Analog telephones or devices cannot use the other Call Park codes.

Attention: Model 7000 phones are supported in Europe only.

Calls are retrieved by pressing the intercom button and dialing the retrieval code. On model 7000 and analog telephones, pick up the receiver, and then dial <parkcode>25.

You also need to program the delay timer that determines when external parked calls that are not answered return to the originating telephone.

You can disable Call Park by setting the Park Code to None.

Public networking—tandem call from private node

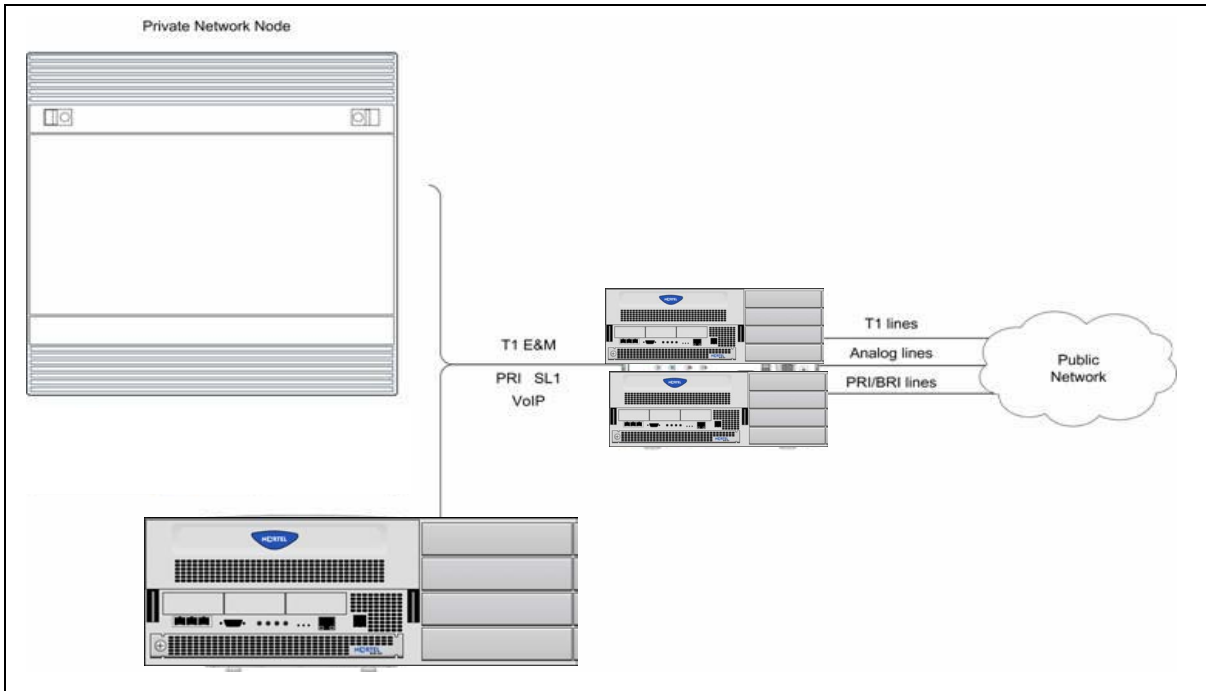
This section provides an overview of tandem calls from a private node.

Tandem calls from a private node

If your system is connected by a private network to another system that does not have PSTN line access, or which is not located within the local dialing range, you can set up a routing plan that allows the users of the private network to dial into your system, and through your system to the PSTN network. This type of call feature is referred to as tandem dialing. Refer to [Configuration for tandem dialing \(page 108\)](#).

The reverse is also true. You can set up routing so that calls from the PSTN can be passed through your system and over the private network to the remote node. Also refer to [Private networking—PRI and VoIP tandem network \(page 125\)](#).

Figure 21 Tandem dialing through a BCM to or from a private network



Configuration for tandem dialing

Since incoming lines terminate within the system, you need to set up routing to pass the calls along to the required destination.

Lines:

- Set up private network lines as auto answer (if applicable).
- Put private and public lines into separate line pools.
- Assign lines to configured Remote Access Packages

Dialing plan/Routing:

- Coordinate Dialing plan with private network node.
- Assign each line pool to a route
- Create destination codes for the private network node, and the public network, using the appropriate routes. On public route, drop the public network access code off the dial string. On the private route, drop the private network access code off the dial string.

Telephones:

- System telephones are not involved in tandem transactions. However, for calls destined for the system, ensure that the telephones have the

appropriate line/line pool assignments to receive calls from both the public and private networks.

Caller access on a tandem network

In this type of configuration, there are three types of callers. Each type of caller has a specific method of accessing the other two systems.

Callers using BCM

These callers can

- call directly to a specific telephone
- select an outgoing line to access a private network
- select an outgoing line to access features that are available on the private network
- select an outgoing central office line to access the public network
- use all of the BCM features

Callers in the public network

These callers use the public lines to

- call directly to one or more BCM telephones
- call into BCM and select an outgoing TIE line to access a private network
- call into BCM and select an outgoing central office line to access the public network
- call into BCM and use remote features

Callers in private network node

These callers use private lines to

- call directly to one or more BCM telephones
- call into BCM and select an outgoing TIE line to access other nodes in a private network
- call into BCM and select an outgoing central office line to access the public network
- call into BCM and use remote features

Private networking—MCDN over PRI and VoIP

The following describes how to network BCMs together in a private network using PRI lines with MCDN protocol. When BCMs are networked with other call services, such as Meridian 1, using the MCDN protocol, the network can also support centralized voice mail.

This chapter discusses MCDN networking based on North American trunks (PRI SL-1). ETSI-QSIG private networking is configured very similarly, although network features may be supported slightly differently.

The following describes the different aspects of MCDN private networking.

- [MCDN used to network with Meridian \(page 111\)](#)
- [Fallback over VoIP MCDN \(page 119\)](#)
- [Networking with ETSI QSIG \(page 120\)](#)

Refer to reference not found for general requirements and directions for setting up non-PRI private networks.

MCDN used to network with Meridian

When you connect your BCM systems through the MCDN protocol to a Meridian 1, the Meridian system manages several aspects of the network, including voice mail, auto attendant services, and system timing.

Programming note: For information about networking voice over IP (VoIP) trunks, which also can be set to use MCDN. For networks running BCM 1.0 software or newer, the trunk protocol for Meridian 1 IPT connection should be set to CSE.

The following information includes how to set up an MCDN network:

- [Meridian system requirements \(page 112\)](#)

Meridian system requirements

When setting up networking with Meridian, the Meridian systems must provide the following:

- provide the correct software version to allow MCDN features. If your Meridian system administrator cannot confirm this, call your technical support center (TSC) or 1-800-4NORTEL
- act as the timing master for the private network connections
- use descending mode for PRI B-channel selection
- recognize dial codes for all nodes in the network
- provide routing tables that direct incoming calls to the correct nodes on the network, including DID calls from the public network
- recognize the destination code (usually 9) that indicates a public network call, regardless of where in the network the number was dialed from

The Meridian must provide the following:

- end-to-end signaling (option 10)
- message center (option 46) and an IVMS link (option 35)
- Meridian Mail link (options 77 and 85)
- basic Attendant Console Directory features (options 40, 45, and 83)
- ISDN PRI or ISDN Signaling link (options 145 and 146 or 145 and 147)
- advanced ISDN features (option 148)
- network message services (option 175)

Meridian software requirements

These additional software packages may be required to activate all the options on the Meridian.

For a new M1 (option 81C, 61C or 51C) on X11 RIs 25, the following additional packages are required to provide the software options listed above:

- SW0059B
- SW0052D
- SW0221C
- SW0051B

For a new M1 Option 11C or 11C Mini or X11 Rel. 25, order one of the following:

- Enterprise software package
- NAS/VNS software package

MCDN call features over PRI SL-1 lines

An MCDN connection with a Meridian 1 voice mail system provides some special call features.

Features for centralized messaging

The following describes the features for centralized messaging:

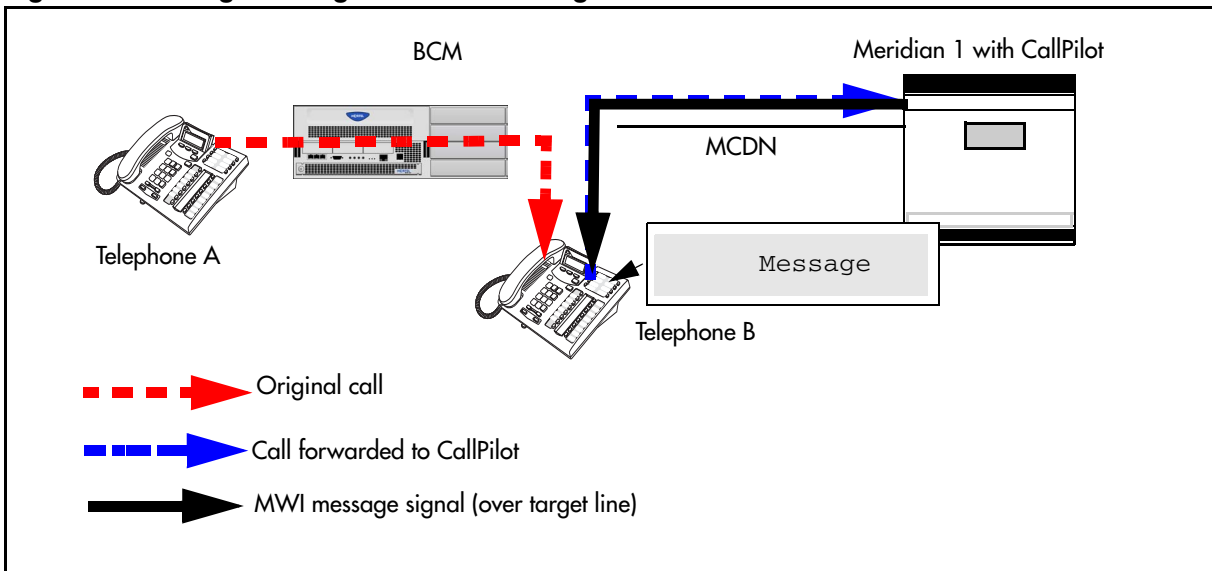
- [Message waiting indication \(page 113\)](#)

Message waiting indication

MWI allows the voice mail host system (Meridian 1) that is designated to receive messages to notify a target telephone on the BCM of a call waiting using the native MCDN MWI or MIK/MCK message indicators on the Meridian telephones. This feature works for both Nortel and third-party voice mail systems. Messages are received at a centralized location, to a predetermined telephone, where they are processed and forwarded to the target telephone.

MWI allows the user to reply or call back to the message center. The procedure for retrieving messages is described in the Telephone Features Handbook.

Figure 22 Message waiting indication message



Features for centralized attendant

The following describes the features for centralized attendant

- [Call camp-on inter-operability \(page 114\)](#)
- [Break-in inter-operability \(page 114\)](#)

Call camp-on inter-operability

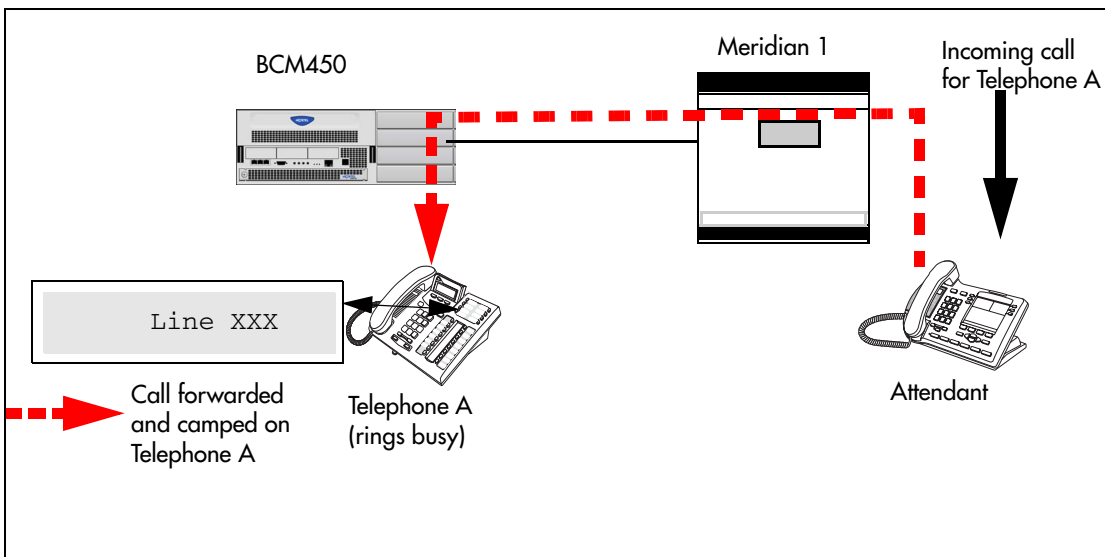
A call received by the Meridian attendant can be assigned to a telephone anywhere in the MCDN network, when the following situations are valid:

- the target telephone rings busy when the attendant calls
- no free keys on target telephone
- DND regular feature is inactive
- DND on busy feature is inactive

The target user sees that there is a call camped on the telephone. The called user can then clear a busy lines and take the call, or the user can choose to reject the call, using F814, or the user can indicate Do Not Disturb, using F85

The following figure demonstrates the call path for a Meridian attendant to camp a call on a telephone in the system.

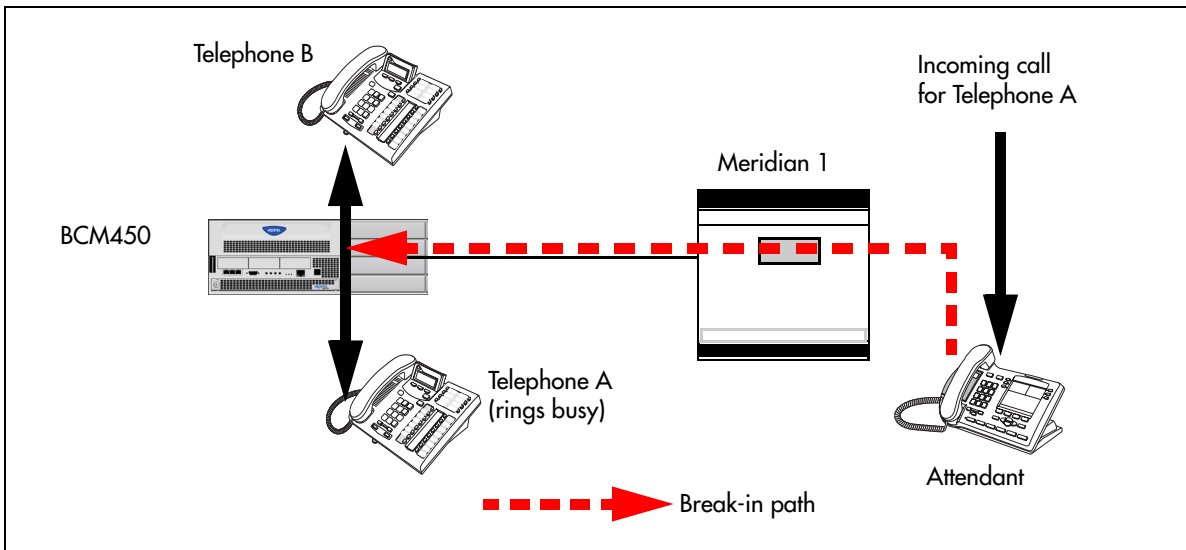
Figure 23 Camping a call



Break-in inter-operability

The Meridian attendant can use the break-in feature to interrupt an ongoing call from a telephone in the system.

The following figure demonstrates the call path for a Meridian attendant to break into a call between telephones in the system.

Figure 24 Breaking into a local system call path

Break-in can occur when these situations are valid:

- Target system telephone is busy but still has a free intercom or line key.
- There is no camped call on the target telephone.
- DND on busy is turned on.
- prime set is also busy, with no free key, and with DND turned on.
- Attendant capability is high (2), and higher than either the target telephone or the caller the target telephone owner is busy with.

Only post-dial break-in is supported by MCDN:

- Attendant dials destination number.
- If a busy tone is heard, the attendant presses the BKI button
Attendant is given access to the conversation.

You can set a level of priority that determines if a telephone allows an attendant to break in. This is referred to as setting the Intrusion level. Use the following rules to configure the break-in feature.

- Set the Intrusion level for each telephone (under Capabilities on the DN record).

How the intrusion hierarchy works:

- Break-in is allowed if Attendant telephone is High and caller telephone is Medium.
- Break-in is not allowed if Attendant telephone is Meridian and caller telephone is high.

UDP-specific programming

The following points provide a quick check for the system prerequisite settings for MCDN networking:

- DNs on the same node are dialed directly
- DNs on other nodes are called by first dialing an Access Code and an ESN
- Each node has its own ESN

BCM UDP programming

Refer to the following table for the information regarding UDP programming.

BCM UDP programming	
Private Dialing Plan:	Type=UDP, HomeLoc=<three-digit prefix>
Private Access Code	<unique code>
Private DN length	<total of Private Access Code + Location Code + DN length> Example: if dialing string is 6 393 2222, then set private DN to 8. Private DN length is for DPNSS private networking only
Program the DestCodes for the other nodes	AccessCode plus the ESN, absorb the AccessCode. Example: For AccessCode=6; DestCode=6393[Absorb=1]

Meridian UDP programming

Refer the following table for Meridian UDP programming.

M1 UDP programming		
Private Access Code	Overlay 86, LD 86 REQ: PRT CUST: 0 FEAT: ESN	To change Private Access Code: Overlay 86, LD 86 REQ: CHG CUST: 0 FEAT: ESN, keep pressing until you reach the AC1 prompt At the AC1 prompt, make your choice

M1 UDP programming	
Check UDP programming	Overlay 90, LD 90 REQ: PRT CUST: 0 FEAT: NET TYPE: LOC LOC: press enter, all the programmed location codes are listed HLOC is the home location of the M1
Program UDP values to route	Overlay 90, LD 90 REQ: CHG CUST: 0 FEAT: NET TYPE: AC1 LOC: (enter a number) RLI: (enter the RLI corresponding to the route)

CDP-specific programming

The following points provide a quick check for the system prerequisite settings for MCDN networking.

- DNs on all nodes are dialed directly

BCM CDP programming

Refer the following table for CDP programming.

BCM CDP programming	
Private Dialing Plan: Private	Type=CDP
Access Code <unique code>.	
Private DN length	<system DN length> Private DN length is for DPNSS private networking only.
PNI	<number assigned from M1 (1-127)>
Program the DestCodes for the other nodes	use Steering code as part of dial string

Meridian CDP programming

Refer the following table for Meridian CDP programming.

M1 CDP programming	
PNI	LD 16, RDB - PNI in M1 programming LD 15 - Net - PNI in M1 programming set to PNI of switch
Distant Steering Codes	Overlay 87, LD 87 REQ: PRT CUST: 0 FEAT: CDP TYPE: DSC (Distant Steering Code) DSC: press enter (lists all DSC programmed)
Check RLI (Route Line Index)	Overlay 86, LD 86 REQ: PRT CUST: 0 FEAT: RLB PLI: press enter (displays all the RLIs)
Program new CDP value to route	Overlay 87, LD 87 REQ: CHG CUST: 0 FEAT: CDP TYPE: DSP DSC: enter number (enter common BCM system number, for example if DNs are 4XX, enter 4) RLI: enter the RLI that corresponds to the route

Meridian 1 programming

The prerequisites for Meridian 1 programming are as follows:

- Program the system PNI and the PNIs for the routes.
- Program the Meridian voice mailboxes (if required).
- Enable the MCDN Supplementary Services: RCAP=[ND2, TRO] or RCAP=[ND2,TRO,MWI], NASA=YES.

VM programming with Meridian 1

If you are using the centralized voice message system from a Meridian 1 system, you require the following programming on the M1:

M1 programming in LD 17

- NASA selected
- NCRD selected

M1 programming in LD 17 NASA selected NCRD selected			
Verifying NASA is Active Overlay 22, LD 22 REQ: PRT TYPE: ADAN DCH (slot number) NASA should be selected			
If NASA is not on:	Disable the D channel Overlay 96, LD 96 REQ: CHG TYPE:DISDCH	Disable the loop Overlay 60, LD 60 REQ: CHG TYPE: DISL (slot number)	Program the D channel Overlay 17, LD 17 REQ: CHG TYPE: ADAN ADAN: CHG DCH (slot number) Keep pressing enter until you get to NASA TYPE: yes TYPE: end
Verifying NCRD Overlay 20, LD 20 REQ: PRT TYPE: TIE CUST: 0 Route: Enter the route defined in LD 20 Keep pressing enter until all values are displayed. Check if NCRD is yes.		If NCRD is set to no Overlay 16, LD 16 REQ: CHG TYPE: RDB CUST: 0 ROUT: (route number) from LD 20 Keep pressing enter until you get NCRD and type Yes Keep pressing enter until you get the REQ prompt again TYPE: end	

Meridian TRO programming

If you are using a Meridian 1 system as part of the network, you need the following programming for each system.

```
M1 TRO set to yes for BCM
route:

LD 16

TYPE: RDB

Cust: xx

Rout: 0-511

TRO: Yes
```

Fallback over VoIP MCDN

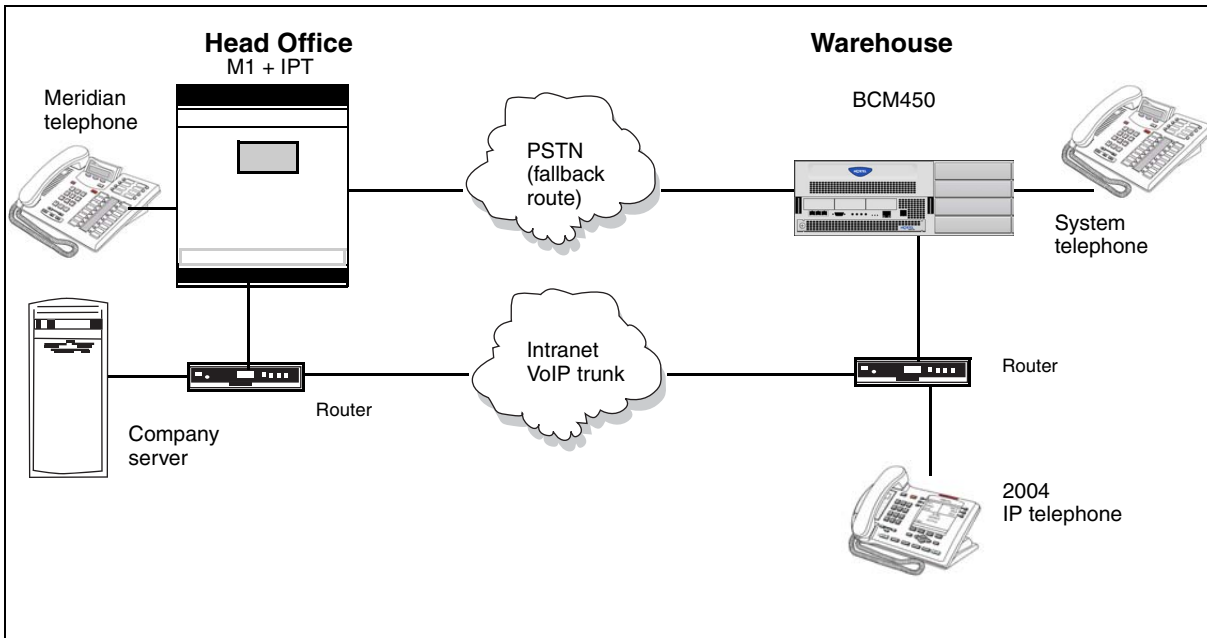
The Voice over IP (VoIP) MCDN networking protocol between a Meridian 1 and one or more BCMs works the same way as it does over PRI lines. You still require the MCDN and IP telephony software keys and compatible dialing plans on all networked systems.

Configuring fallback over VoIP MCDN network

The one difference between MCDN over PRI and MCDN over VoIP is that the VoIP trunks require specific Remote Gateway settings, unless there is a Gatekeeper configured to route traffic on the IP network. You must also ensure that your line is a PRI SL-1 line, to maintain MCDN features on the network.

Refer to the following figure for an example.

Figure 25 M1 to BCM network diagram



MCDN functionality on fallback PRI lines

To enable MCDN functionality over PRI fallback lines

- Check MCDN PRI settings on the M1. For information on this, refer to the M1 documentation.
- Ensure SL-1 (MCDN) keycodes are entered on the BCM and the PRI line is set up for SL-1 protocol

Networking with ETSI QSIG

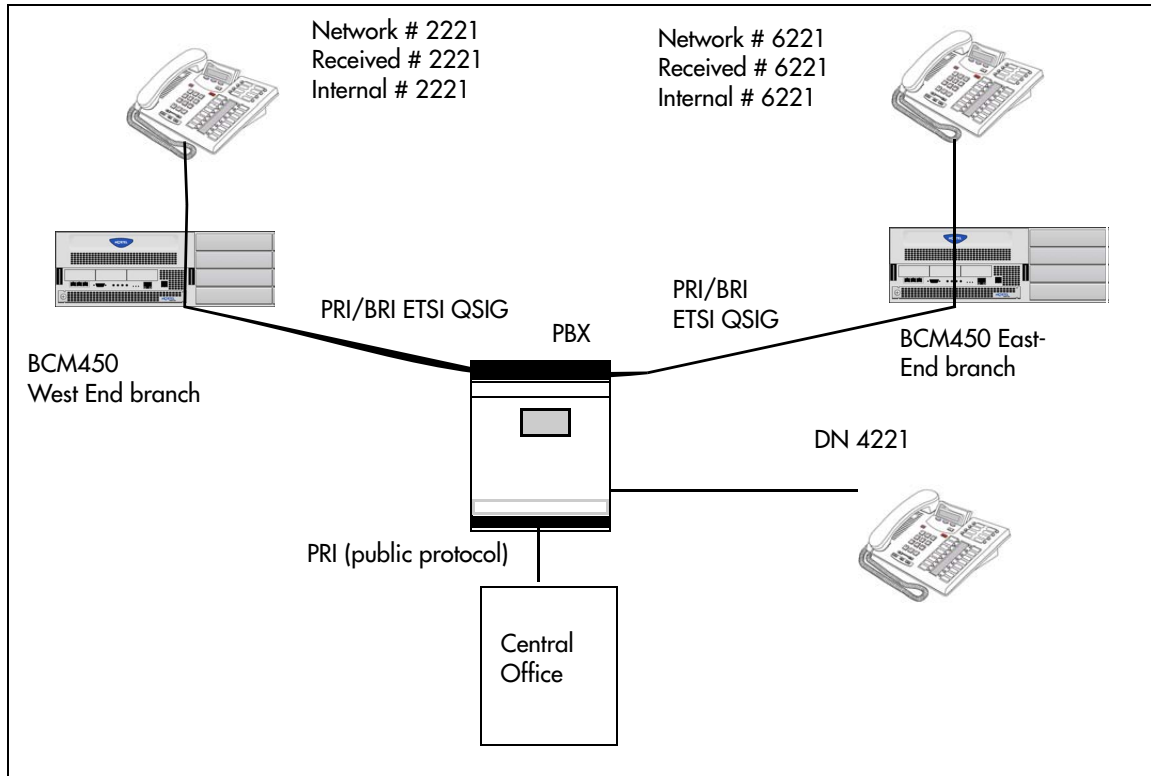
ETSI QSIG is the European standard signaling protocol for multi-vendor peer-to-peer communications between PBX systems and/or central offices.

Networking with ETSI QSIG

The following figure illustrates an ETSI QSIG network.

Attention: Features for ETSI Q.sig are basic compared to MCDN. Only basic call and calling number is supported as opposed to the many MCDN features.

Figure 26 ETSI QSIG networking



Settings for some of the hardware parameters for the ETSI QSIG networking example shown above are as follows.

West End office:			East End office:		
Hardware programming	DTM/BRIM	PRI/BRI	Hardware programming	DTM/BRIM	PRI/BRI
	Protocol	ETSI QSIG		Protocol	ETSI QSIG
	BchanSeq	Ascend (PRI only)		BchanSeq	Ascend (PRI only)
	ClockSrc	Primary		ClockSrc	Primary

Private networking—MCDN and ETSI network features

This section gives an overview of the MCDN and ETSI network features in private networking.

MCDN network features

When you connect your BCM systems through PRI SL-1 or VoIP trunks and activate the MCDN protocol, your network provides a number of network call features. You can use this protocol to network other BCM systems, Norstar systems, Meridian 1 systems, Succession systems, and DMS-100 systems.

ISDN call connection limitation

The ICCL feature piggybacks on the call initiation request and acts as a check at transit PBX points to prevent misconfigured routes or calls with errors from blocking channels.

Trunk route optimization

TRO finds the most direct route through the network to send a call between nodes. This function occurs during the initial alerting phase of a call.

ETSI Euro network services

If your system has ETSI Euro BRI/PRI lines, you can activate the malicious call identification (MCID) and Network Diversion features. Advice of Charge-End of Call (AOCE) is active if your service provider has activated that service on the line.

When the features are activated, users can:

- display a call charge
- redirect calls over the ETSI Euro BRI/PRI line to the outside network
- tag malicious calls

Advice of Charge-End of Call (AOCE) — AOCE is a supplementary service available from your service provider on ETSI Euro BRI/PRI links. With this feature, the BCM user can view the charges for an outgoing call once the call

completes. This information is also reported to the Call Detail Reporting Application. The information can be provided in currency or charging units, depending on how the feature is set up by your service provider.

To invoke the feature, the user presses FEATURE 818.

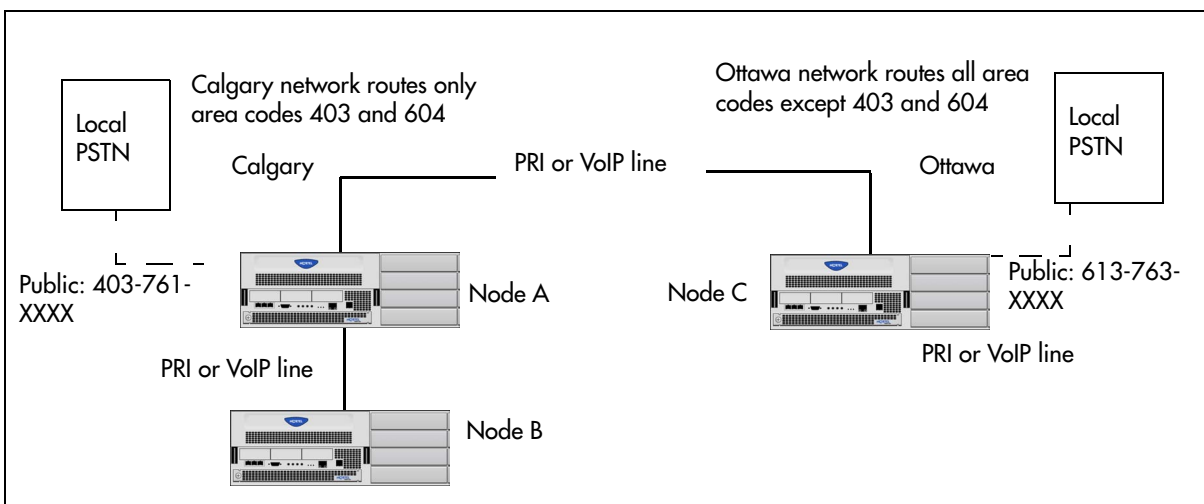
Private networking—PRI and VoIP tandem network

This section gives an overview of PRI and VoIP tandem network. You can use PRI trunks and VoIP trunks to create a private network between other BCMs.

PRI and VoIP tandem configurations

The following figure demonstrates a tandem configuration.

Figure 27 Private tandem network of BCMs



Routing for tandem networks

In this type of network, each Business system node is set up to route calls internally as well as to other nodes on the system. Each node must have a unique identification number, which is determined by the type of dialing plan chosen for the network.

VoIP trunks require local gateway configuration and either remote gateway or Gatekeeper configurations that identify the other nodes in the network.

If the node is also connected to the public network, the usual routing is required for that connection.

The following tables show the routing tables for Node A and Node C for external and internal terminating calls.

Table 26 Node A destination code table, external termination

Route	Absorb length	Destination code (public DNs)
4(PSTN)	1	91604
3(NodeB)	0	91403762 (Node B)
4(PSTN)	1	9140376* (not internal network)
4(PSTN)	1	914037* (not internal network)
4(PSTN)	1	91403* (not internal network)
4(PSTN)	1	9* (not internal network)
* This wild card represents a single digit.		

Table 27 Node A destination code table, internal termination

Route	Absorb length	Destination code (private DNs)
3(Node B)	0	392 (Node B)
5(Node C)	0	393(Node C)

Table 28 Node C destination code table, external termination

Route	Absorb Length	Destination code (Public DNs)
3(Node B)	0	91613764 (Node D)
3(node B)	0	91613766 (Node F)
4(PSTN)	1	9161376* (not internal network)
4(PSTN)	1	916137* (not internal network)
4(PSTN)	1	91613* (not internal network)
4(PSTN)	1	9161* (not internal network)
4(PSTN)	1	916* (not internal network)
4(PSTN)	1	91* (not internal network)
4(PSTN)	1	9 (not internal network)

Table 29 Node C destination code table, internal termination

Route	Absorb length	Destination code (Private DNs)
5(Node A)	0	391(Node A)
5(Node A)	0	392(Node B)

Call progress through tandem networks

The following provides a step-by-step description of how calls network through a tandem network:

- [Calls originating from public network \(page 127\)](#)
- [Calls originating within private network \(page 128\)](#)

Calls originating from public network

The following table describes how each node handles calls originating from the public network into the system.

Table 30 Call originating from the public network to a tandem network

Original receiving node	Destination node	Description
Node A	Node A	User in Calgary on the PSTN dials 761-xxxx number Incoming interface: Public DN type: Public Node A receives the call and identifies it as terminating locally. Uses target line to route call (Public received #). Destination: Local (target line)
Node A	Node B	User in Calgary on the PSTN dials a 762-xxxx number DN type: Public Node A receives it and identifies it as being for node B. Uses private trunk to route it to B. Incoming interface: Public Destination: Remote Node Outgoing interface: Private DN type: Private Node B receives the call and identifies it as terminating locally. Uses target line to route call (Private received #). Incoming interface: Private Destination: Local (target line)

Table 30 Call originating from the public network to a tandem network

Original receiving node	Destination node	Description
Node A	Node C	<p>An external user in Calgary dials a 761-xxxx number which is answered with DISA. Incoming interface: Public DN type: Public Destination: Local (DISA DN)</p> <p>User enters a CoS password and a private DN for Node C 6 + 393-xxxx DN type: Private</p> <p>Node A receives it and identifies it as being for C. Uses the private trunk to route the call to C. Incoming interface: (DISA user) Destination: Remote node</p> <p>Node C receives the call and identifies it as terminating locally. Uses target line to route call. (Private received #) Incoming interface: Private Destination: Local (target line)</p>
Node A	Ottawa PSTN	<p>An external user in Calgary dials a 761-xxxx number which is answered with DISA. User enters a CoS password and an Ottawa public network number. Incoming interface: Public DN type: Public Destination: Local (DISA DN)</p> <p>Node A receives it and identifies it as being for C. Uses the private trunk to route the call to C. Incoming interface: Local (DISA user) Destination: Remote PSTN</p> <p>Node C receives the call and identifies it as a public number and routes it out over the local PSTN. Incoming interface: Private Destination: Local PSTN</p>

Calls originating within private network

The following table describes how each node handles calls originating in the public network.

Table 31 Calls originating from the private network within a tandem network

Original receiving node	Destination node	Description
Node B	Node B	DN is internal, therefore no trunk routing is required. Incoming interface: Intercom DN type: Local Destination: Local
Node A	Ottawa PSTN	User in Node A dials the private network access code for Node C, followed by an Ottawa public number. Incoming interface: Intercom DN type: public Destination: Remote PSTN Node C receives the call and identifies it as being for the public network. Node C routes the call over the local public network. Incoming interface: Private DN type: Public Destination: Local PSTN
Node B	Calgary PSTN	User on Node B dials a public DN. Node B recognizes it as being the responsibility of Node A and uses private trunk to route the call to A. Incoming interface: Intercom Destination: Remote node Node A receives the call and identifies it as being for the public network. Node A routes the call over the local public network. Incoming interface: Private Destination: Remote PSTN

Table 31 Calls originating from the private network within a tandem network

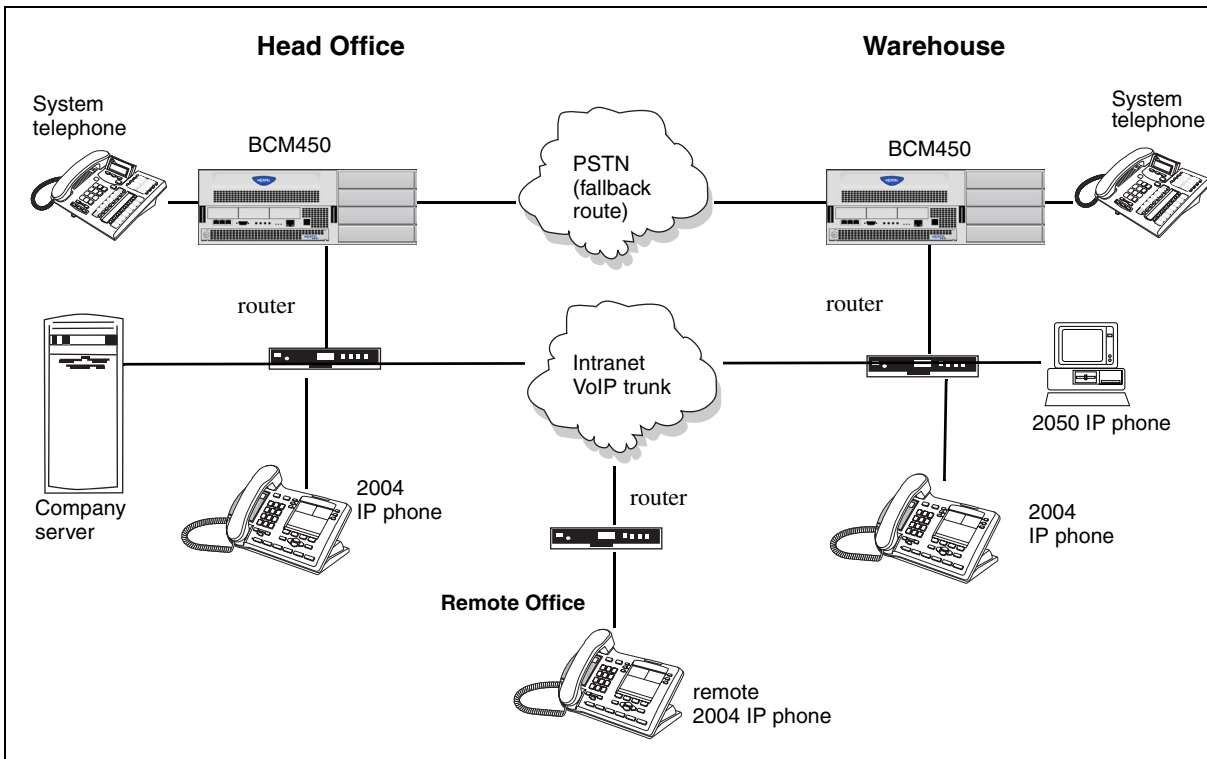
Original receiving node	Destination node	Description
Node B	Node A	<p>User in Node B dials a private DN for a user on A. DN type: Private</p> <p>Node B recognizes it as being for Node A. Uses the private trunk to route the call the call to A. Incoming interface: Intercom Destination: Remote node</p> <p>Node B receives the call and identifies it as terminating locally. Uses target line to route call. (Private received #) Incoming interface: Private Destination: Local (target line)</p>
Node B	Node C	<p>User on Node B dials a private DN for a user on C. DN type: Private</p> <p>Node B recognizes it as being the responsibility of Node A and routes the call over the private trunk to A. Incoming interface: Intercom Destination: Remote node</p> <p>Node A receives it and identifies it as being for C. Uses IP trunk to route call to C. Incoming interface: Private Destination: Remote node</p> <p>Node C receives the call and identifies it as terminating locally. Uses target line to route call. (Private received #) Incoming interface: Private Destination: Local (target line)</p>

VoIP to tandem systems

You can connect multiple offices with BCMs across your company intranet. With this installation CallPilot directs calls throughout the system or for one system to support voice mail for the network. Full toll bypass occurs through the tandem setup, meaning that any user can call any DN without long distance charges being applied. Users have full access to system users, PSTN connections.

Private network with multiple BCMs

The following figure demonstrates a multiple-BCM450 network. The network diagram shows two BCMs, but additional base units can be added.

Figure 28 Multiple BCMs network diagram**BCM network setup**

When setting up a network of BCMs

- Ensure that the existing network can support the additional VoIP traffic.
- Coordinate a Private dialing plan between all the systems.
- On each BCM
 - Set up outgoing call configuration for the VoIP gateway.
 - Set telephones to receive incoming calls through target lines.
 - Configure the PSTN fallback and enable QoS on both systems.

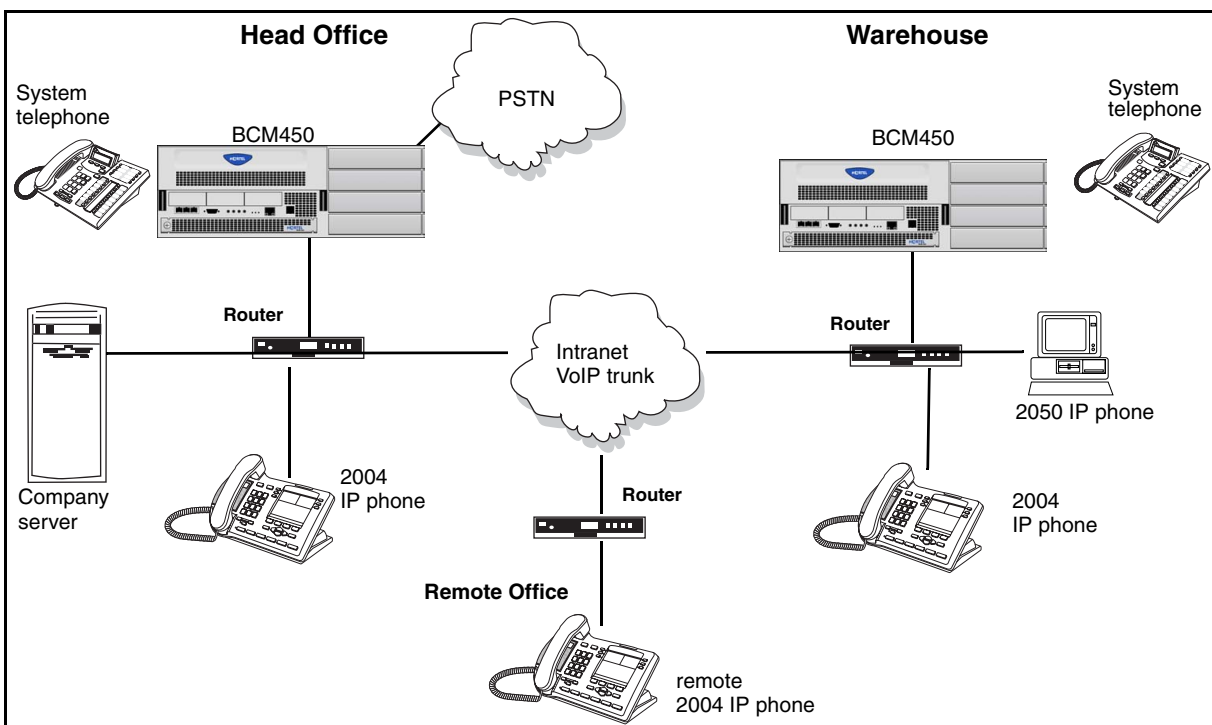
This system uses fallback to PSTN so calls can be routed across the PSTN connection if VoIP traffic between the BCMs becomes too heavy.

If only one of the BCMs in a network has a line to the PSTN network, all public calls from other systems are funneled through the system with the PSTN connection, and all communication between the systems occurs over VoIP trunks. To facilitate this system, you need to ensure that the destination codes on the non-PSTN system point to the system connected to the PSTN, and then, to the PSTN. On the PSTN-connected system, the system and destination codes must be configured to recognize and pass public calls from the other system out into the PSTN network. Since the receiving PSTN sees the calls as remote dial-ins, ensure that the correct remote access packages have been established for the VoIP trunks.

This also means that if the VoIP trunks are inaccessible between the systems, there is no provision for a fallback route.

The following figure demonstrates an example of routing all public calls through one BCM450.

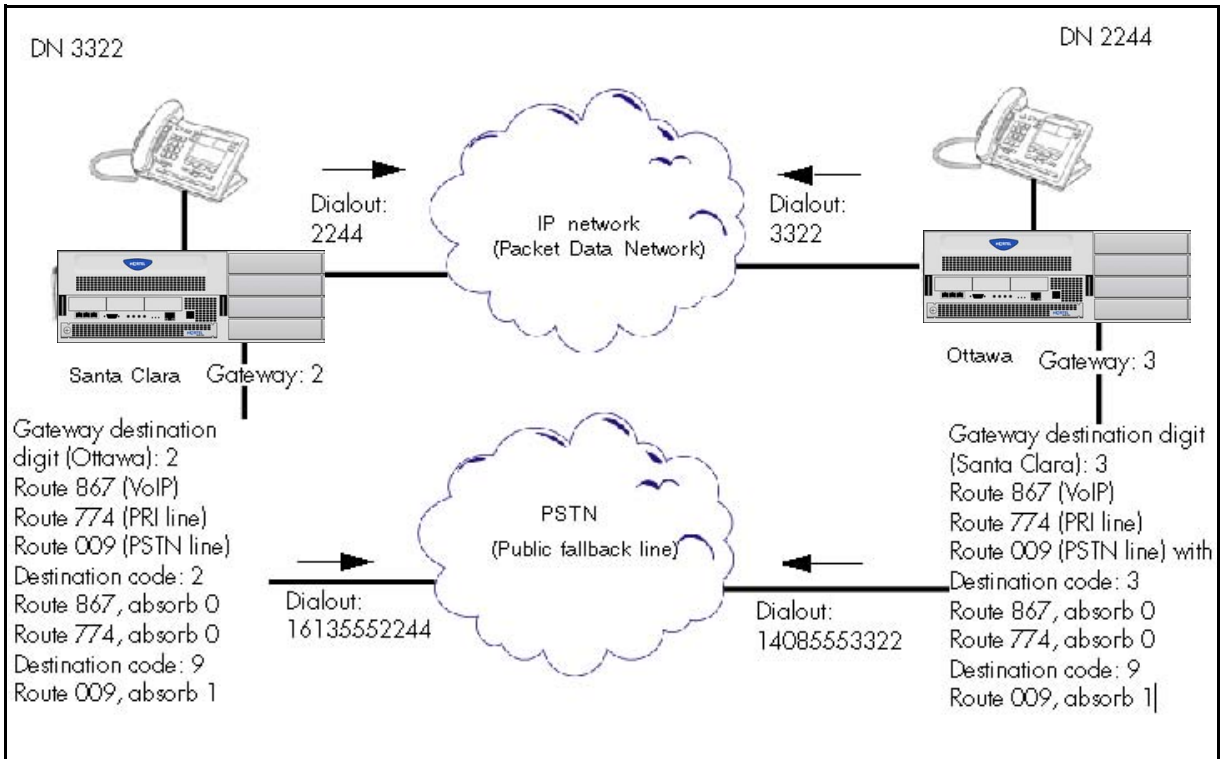
Figure 29 Routing all public calls through one BCM



Example of a private network configured for fallback

The following describes a sample BCM configuration. In this scenario, shown in the following figure, two BCMs in different cities are connected through a WAN.

One BCM is in Ottawa, the other is in Santa Clara. Both VoIP trunks and an PRI SL-1 line connect the system in a private network.

Figure 30 Example PSTN fallback

Private networking—DPNSS network services (UK)

This section provides an overview of DPNSS network services.

The following features are available and can be programmed over DPNSS lines:

- Diversion ([DPNSS diversion feature \(page 135\)](#))
- Redirection ([DPNSS redirection feature \(page 137\)](#))
- [Executive intrusion \(page 137\)](#)
- [Call offer \(page 138\)](#)
- [Route optimization \(page 139\)](#)
- [Loop avoidance \(page 140\)](#)
- MWI is discussed with central voice mail setup [Centralized voice mail \(page 159\)](#)

DPNSS diversion feature

Diversion is a DPNSS 1 feature for BCM that allows users to forward their calls to a third party on the DPNSS 1 network. This feature is similar to call forward on BCM, but takes advantage of the broader capabilities of DPNSS.

There are five variations of Diversion: Call Diversion Immediate, Call Diversion On Busy, Call Diversion On No Reply, Bypass Call Diversion, and Follow-me Diversion. These variations are described in the following list:

- Diversion Immediate diverts all calls to an alternate telephone. This function is programmed by the user at their telephone.
- Diversion On Busy diverts all calls to an alternate telephone when a telephone is busy. This feature is programmed in the Element Manager.
- Diversion On No Reply diverts calls that go unanswered after a specified amount of time. This feature is programmed in the Element Manager.
- Bypass Call Diversion overrides all call forward features active on a telephone over a DPNSS line.

- An incoming call to the telephone cannot be forwarded; instead, the telephone continues to ring as if call forward were not active. This feature is used to force a call to be answered at that location. Bypass Call Diversion is a receive-only feature on BCM, and cannot be used from a BCM telephone.
- Follow-me Diversion is also a receive-only feature. It allows the call forwarded destination to remotely change the BCM call-forwarding programming (Call Forward All Calls (CFAC) feature) to a different telephone.

Attention: BCM CFAC must be active, and the destination set/PBX system must support the feature.

For example, user A forwards all calls to telephone B, a temporary office. Later, user A moves on to location C. The user does not have to be at telephone A to forward calls to location C. Using telephone B and Follow-me Diversion, the user can forward calls from A to location C

Follow-me diversion can be cancelled from the forwarded location.

- Diversion on Busy and Diversion on No Reply cannot be cancelled from the forwarded telephone. These are programmable only by an installer and not by the user.
- If multiple telephones are programmed to take a call, the first telephone to respond acts. All other telephones responding are ignored. Therefore, if the first telephone to respond has Diversion enabled, this feature is invoked.

Diversion feature

You set Diversion for DPNSS in the same way as call forward. You must enter the end DN when prompted. You may also need to include the DPNSS 1 routing number.

DPNSS diversion configuration

DPNSS lines connected to an Embark switch perform call redirection/diversion using the Call Forward feature to create a tandem link back to the switch. Since this is different from other switches, you must select the type of switch DPNSS connects to when you do module programming. For information on configuring trunk module parameters, see *Nortel Business Communications Manager 450 1.0 Configuration—System* (NN40160-501).

Before you program Call Forwarding ensure that:

- Both real channels and virtual channels are provisioned.
- Destination or line pool codes are programmed for the DPNSS to Embark link. Also, during programming for Call Forward No Answer and Call Forward on Busy, when you enter the Forward to: digits, the system does a validation check with the switch on the number. (Configuration > Telephony > Sets, All DNs panel, Line Access tab, and then double-click the required field to enter the DN).

DPNSS redirection feature

Redirection is a DPNSS 1 feature similar to BCM Transfer Callback. With Redirection, the originating party can redirect a call awaiting connection, or re-connection, to an alternate destination after a time-out period. Failed calls can also be redirected. Priority calls are not redirected.

Call restrictions by set type

The call restrictions by set type are as follows:

- For telephones with single line displays, the # key acts as MORE and the * key acts as VIEW
- ATA2/ASM8+—not supported
- ISDN—all variations supported on ISDN telephones

Redirection configuration

The timer used for the network Callback feature is also used for redirection.

Executive intrusion

Executive Intrusion (EI) is a DPNSS 1 feature that allows an operator, or other calling party, to intrude on a line when it is busy. An example of the use of this feature is to make an important announcement when the recipient is on another call.

Executive intrusion implementation

EI is implemented on the BCM using Intrusion protection level (IPL). IPL has four settings, from None to High. A telephone set has the ability to break-in when the other telephone set has a lower IPL. The default setting is None and a setting of High prevents intrusion.

EI is similar in functionality to BCM Priority Call, but it is a receive-only feature on BCM telephones. EI cannot be initiated from a BCM telephone. The person using this feature must be on another PBX system on the DPNSS 1 network.

When EI is used to intrude on a call in progress, a three-way connection is established between the originating party and the two parties on the call. The result is very much like a conference call. When one of the three parties clears the line, the other two remain connected, and EI is terminated.

Call restrictions by set type

The call restriction by set type areas follows:

- ATA2/ASM8+—supported
- ISDN—not supported

The telephone receiving the intrusion displays Intrusion Call. A warning indication tone sounds after intrusion has taken place, and the standard conference call tone sounds every 20 seconds.

Call offer

Call Offer over DPNSS 1 allows a calling party to indicate to the wanted party that there is an incoming call available, even though there is no answer button available to present the call on the telephone. The intended recipient can ignore, accept, or decline the offered call. Call Offer is useful in increasing the call-coverage capability of a BCM system, and helps to lift the network processing load. It is a receive-only capability on BCM; incoming calls are initiated at another PBX system on the DPNSS 1 network.

An example of Call Offer in use is an operator or attendant who has a number of calls coming in at once. The operator can call offer one call and move to the next without waiting for the first call to be answered.

Call offer displays

When a Call Offer is made by the originating exchange, the target telephone displays a message, and a tone is heard. When an offered call arrives on telephones with line display, the user sees XX...X wtng if the calling party ID is available and CLID is enabled. If CLID is not available or CLID is disabled, Line XXX waiting appears (the line name associated with the call). If there are more than 11 digits in the incoming number, only the last 10 display.

If Call Queuing is programmed for the system, the display shows Release Line XXX. This is the line name of the highest-priority queued call if it is an offered call.

Call offer restrictions by set type

The call offer restrictions by set type are:

- model 7000 telephone — associated LED or LCD flashes, and a tone is heard

- ATA2/ASM8+ —Call Offer is supported as a Camp On feature, and a tone is heard
- ISDN—not supported
Note the following general conditions and restrictions:
 - DND on busy must be programmed as N (DN ##/Capabilities) for a telephone to accept Call Offer.
 - If CF on busy is programmed for the telephone, Call Offer is not accepted.
 - The target line for the telephone must be set to: If busy: busy tone, which is the default. Refer to [Target line configuration \(page 15\)](#).
 - Call Offer does not work if sent over Manual answer lines. It is recommended that the lines be left at the default: **Auto**.

Attention: Forward on Busy takes priority over DND on Busy. Call Offer cannot be accepted by putting an active call on hold.

User actions

The party receiving a Call Offer has three choices:

- Ignore it. After a programmed time interval, the Offer request is removed.
- Reject it. If the user activates Do Not Disturb on Busy (DND) when the Call Offer request is made, the request is removed from the telephone. The calling party is informed of the rejection.

Attention: A call cannot be offered to a telephone with DND active. The line indicator for external incoming calls still flashes.

- Accept it. The Offer is accepted by releasing the active call.

Attention: Forward on Busy takes priority over DND on Busy. Call Offer cannot be accepted by putting an active call on hold.

Route optimization

Route Optimization is a DPNSS 1 feature for BCM that allows calls to follow the optimum route between two end PBXs. This allows efficient use of network resources.

No system programming is required for the feature when BCM is working as a terminating PBX system. However, BCM must have a private access code programmed that maps to a valid destination code or line pool code on DPNSS lines. Further, Allow redirect must be set to selected.

Loop avoidance

Errors in the configuration of a network may make it possible for a call to be misrouted, and arrive at a PBX system through which it has already passed. This would continue, causing a loop which would eventually use up all of the available channels. The Loop Avoidance service permits counting of DPNSS 1 transit PBXs and rejecting a call when the count exceeds a predetermined limit.

Private networking with DPNSS

DPNSS supports the Universal Dialing Plan (UDP), an international standard for sending and receiving private numbers over networks. The UDP requires that a dialing number includes the following:

- a Private Access Code, programmed into the system as part of the destination code table to prevent conflicts with the internal numbering system. (Configuration > Telephony > DialingPlan > Private Network > Private Access Code).
- a Home Location Code (HLC) assigned to each PBX system, and configured as part of the destination code (a maximum of seven digits). For each HLC, a destination code must be programmed in the system. (Configuration > Telephony > Dialing Plan > Private Network > Location code).
- a Directory Number (DNs) assigned to each extension as a line appearance. The DN appears as the last string segment in a dialed number. In the number 244-1111, 1111 is the DN.

A typical Private Number, using a private access code and dialed from another site on the network, appears in the following table.

Private Access Code	+ Home Location Code	+ Directory Number	= Calling Party Number
6	+848	+2222	= 6-848-2222

In this networking example, a private network is formed when several systems are connected through a Meridian M1 and a terminating BCM system. Each site has its own HLC and a range of DNs. The following figure illustrates this example.

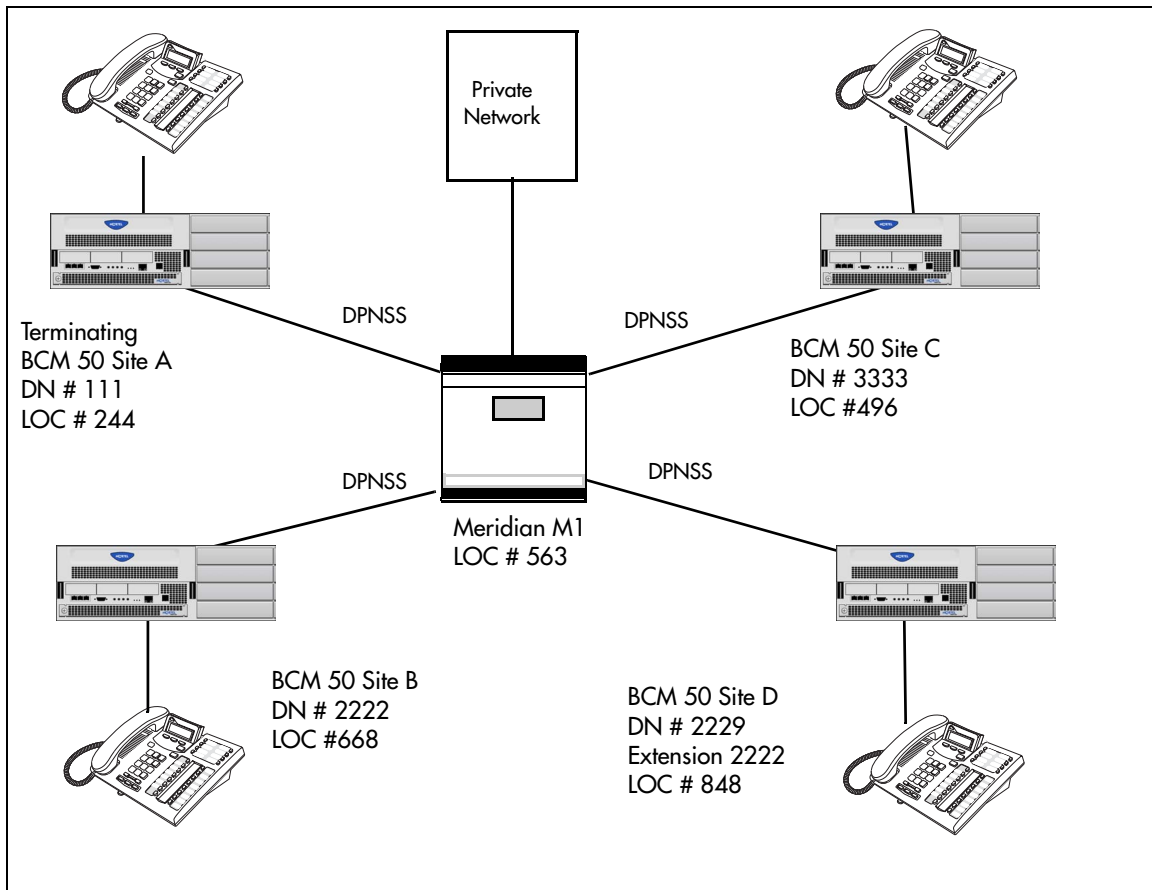
Calls are dialed and identified to the system as follows:

- To reach a telephone inside the Private Network, at the BCM site, the user dials the DN of choice.
- To reach a telephone inside the Private Network, from another site, the user dials HLC + DN.
- To reach a telephone outside the Private Network, the user dials an Access Code + HLC + DN
Each node has its own destination (dest) codes which includes the appropriate access and HLC codes to route the call appropriately.

The following table shows examples of the construction of numbers used when dialing within the example network. Note that 6 is the Private Access code.

Table 32 Calling numbers required for DPNSS network example

Calling Site	LOC/HLC	LOC/HLC Calling Party Number	Called Site	Dialing String	Called Party Number
Site A	244	244 1111	Site B	6 668 2222	668 2222
Site B	668	6 668 2222	Site D	6 848 2222	848 2222
Site D	848	2222	Site D	2229	2229
Site C	496	496 3333	Public DN	9 563 3245	563 3245

Figure 31 DPNSS networking

The following table shows examples of the routing required to set up the network shown in the figure. Note that 6 is the Private Access code.

Table 33 Routing for DPNSS network

Private Network: (for each branch BCM)			
Routing service to		Private network	Public network
	Route	001	002
	Dial out #	No number	No number
	Use	Pool N	Pool N
	DN type	none (private access code 6 is programmed)	public
	Destination Code	6	9

Table 33 Routing for DPNSS network

Private Network: (for each branch BCM)			
Routing service to		Private network	Public network
	Normal route	001	002
	Absorb	1	1

Custom DPNSS routing service

You can customize the routing service using the following restrictions:

- Direct Inward Access (DIA) lines allow incoming calls on private circuits to be directed to telephones without going through the normal call reception. Each DIA line is assigned to one or more extensions and is given a distinct Private Received number. When someone on another system on the network dials the Private Received number on a DPNSS line, the BCM system checks all received digits, compares the digits to an internal table and routes the call to the appropriate DIA line. All extensions programmed to have access to that DIA line then alert for the incoming call.
- Dialing restrictions can be added to lines in line pools. Filters can restrict the use of the line to specific area codes.
- You can use host system signaling codes () as part of the dial out for a route. Routing can also be used as an alternate method for a direct-dial digit. For example, create a destination code 0 and program the number of the internal or external destination as the dial out. Digit absorption should be set to 1. Because overflow routing directs calls using alternate line pools, a call may be affected by different line restrictions when it is handled by overflow routing.

DPNSS private networking

The Digital Private Network Signaling System (DPNSS 1) is a networking protocol enhancement that extends the private networking capabilities of existing BCM systems. It is designed to offer greater centralized functionality for operators, giving them access to BCM features over multiple combined networks.

Attention: The DPNSS feature is dependent on which region loaded on your system at startup and that a software keycode was entered to enable the feature.

DPNSS 1 allows a BCM local node, acting as a terminating node, to communicate with other PBXs over the network. For example, corporate offices separated geographically can be linked over DPNSS 1 to other BCM

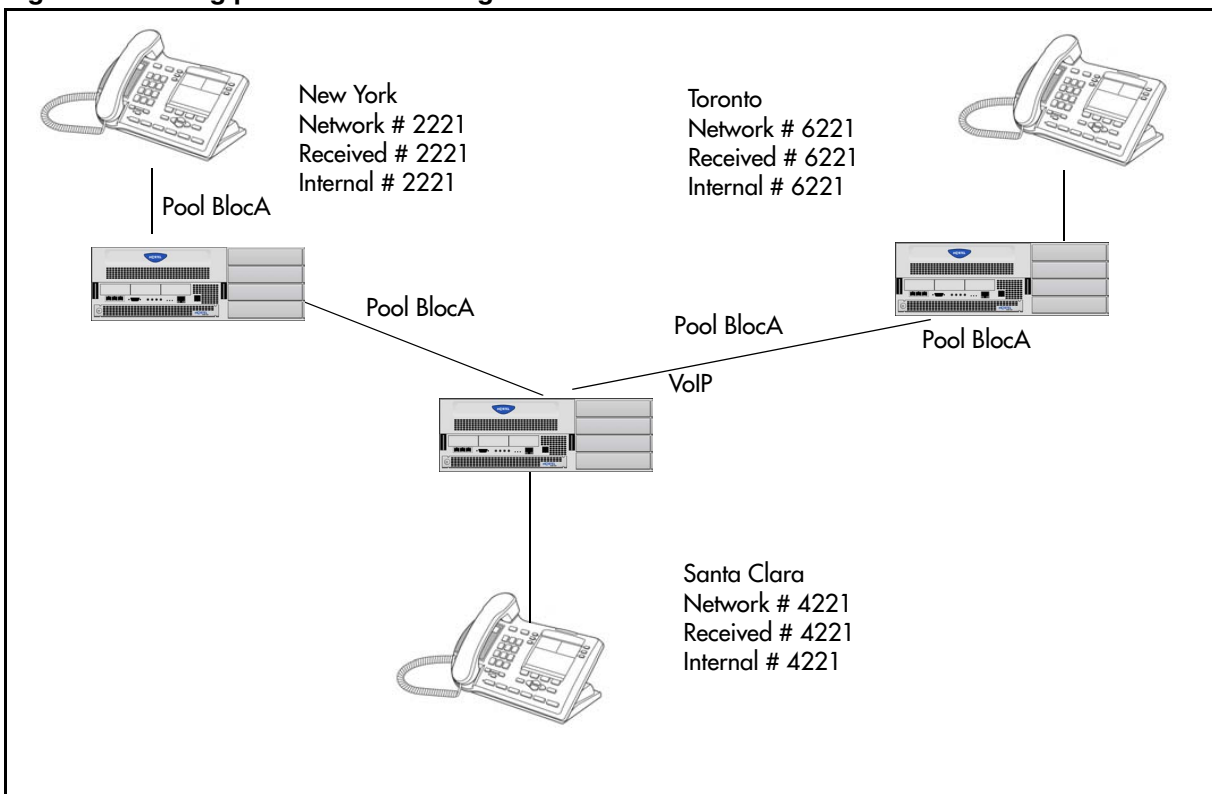
nodes, bypassing the restrictions of the PSTNs to which they may be connected. Connected BCM nodes can therefore function like a private network, with all features of BCM accessible.

You can use DPNSS 1 features on any BCM telephone. On most BCM telephones, you must use specific keys and/or enter a number code to access the features.

Private network—Destination codes

This section gives an overview of destination codes in a private network. By properly planning and programming routing tables and destination codes, an installer can create a dialing plan where VoIP lines between BCM are available to other systems in the network. The following figure shows a network of three BCMs. Two remote systems connect to a central system.

Figure 32 Dialing plan for VoIP routing network



Destination codes in BCM450

Each system must be running BCM software. Each system must be equipped with target lines and a VoIP keycode with at least one IP Trunk line. Programming information for this network is shown in the following table.

Table 34 VoIP routing for a BCM network

New York office:		
Parameter	Setting	
Line Programming		
Network line (external)		
Line 001-004	VoIP	
Line type	BlocA	
Target line (internal)		
Line 125	Target line	
Private Received #	2221	
Line Access (set)		
Set 2221	L125: Ring only	
Line pool access	Line BlocA	
Routing service		
Route	001	
Use	BlocA	
External #	None	
Routing Destinations	Office #1	Office #2
Routing to	Santa Clara	Toronto
Destination Code	4	6
Normal route	001	001
Absorb	None	None
Dialed number:	4221	6221
Santa Clara office:		
Parameter	Setting	
Network line (external to New York)		
Line 001-004	VoIP	
Line type	BlocA	
Target line (internal to Santa Clara telephone)		
Line 125	Target line	
Private Received #	4221	
Line Access		
DN 4221	L125: Ring only	

Table 34 VoIP routing for a BCM network

New York office:			
Parameter		Setting	
	Line pool access	Line BlocA	
Routing Destinations		Office #1 and #2	
Routing to		New York/Toronto	
Route		001	
Use		BlocA	
External #		None	
Destination Code		2	6
Absorb		None	None
Normal route		001	001
Remote access			Note: All lines in BlocA and BlocB need to be assigned in Remote Access Package 1. This is done under the restrictions tab of the lines.
	Rem access pkgs	01	
	Line pool access	BlocA: ON	
	Line pool access	BlocB: ON	
Toronto office:			
Parameter		Setting	
Trunk/Line Data (external)			
	Line 001-004	VoIP	
	Line type	BlocA	
Target line (internal)			
	Line 125	Target line	
	Private Received #	6221	
Line Access			
	DN 6221	L125: Ring only	
	Line pool access	Line BlocA	
Routing Destinations		Office #1	Office #2
Routing to		New York	Santa Clara
Route		001	
Use		BlocA	

Table 34 VoIP routing for a BCM network

New York office:		
Parameter	Setting	
External #	None	
Destination Code	4	2
Absorb	None	None
Normal route	001	001

If a user in New York wants to call Toronto within the network, they dial 6221. The local BCM checks the number against the routing tables and routes the call according to the destination code 6, which places the call using Route 001.

The call appears on the routing table on the BCM in Santa Clara as 6-221. Because 6 is programmed as a destination code for Toronto on the Santa Clara system, another call is placed using route 001 from Santa Clara to Toronto. At the Toronto system, the digits 6-221 are interpreted as a target line Private received number. The call now alerts at telephone 6221 in Toronto.

Attention: Network calls that use routes are subject to any restriction filters in effect.

If the telephone used to make a network call has an appearance of a line used by the route, the call moves from the intercom button to the Line button. The telephone used to make a network call must have access to the line pool used by the route.

Network calls are external calls, even though they are dialed as if they were internal calls. Only the features and capabilities available to external calls can be used.

When programming a button to dial a Network number automatically (autodial), network calls must be treated as external numbers, even though they resemble internal telephone numbers.

Routes generally define the path between your BCM and another call server in your network, not other individual telephones on that call server.

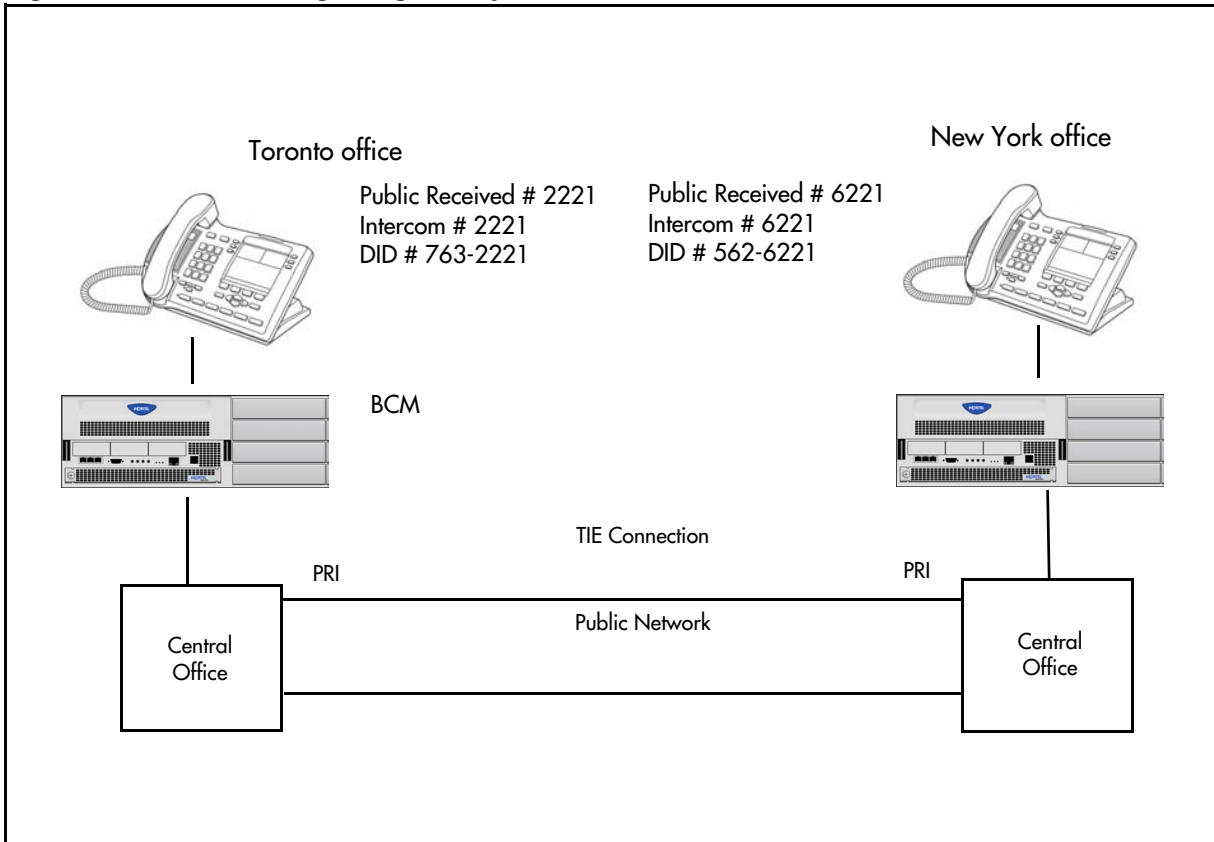
Private networking–PRI call-by-call services

This section gives an overview of PRI call-by-call services in a private network.

The example shown in the following figure highlights the use of PRI Call-by-Call services. It shows two offices of a company, one in New York and one in Toronto. Each office is equipped with a BCM and a PRI-NI2 line. Each office must handle incoming and outgoing calls to the public network. In addition, employees at each office often have to call colleagues in the other office.

Call-by-Call Services must be provided by the Central Office for them to work in the BCM.

Figure 33 PRI networking using Call-by-Call Services



PRI call-by-call services

If Call-by-Call services were not used, each BCM system might have to be equipped with the following trunks:

- 12 T1 DID lines needed to handle peak incoming call traffic
- eight T1 E&M lines needed to handle inter-office calls
- eight lines needed to handle outgoing public calls

The total required is thus 28 lines. If the BCM systems were using T1 trunks, then two T1 spans would be required at each office. Note that the total of 28 lines represents the worst case value for line usage. In reality, the total number of lines in use at any one time is generally less than 28. For example, during periods of peak incoming call traffic, the demand for outgoing lines is low.

Benefits of call-by-call services

With PRI Call-by-Call services, it is not necessary to configure a fixed allocation of trunks. Each of the 23 lines on the PRI can be used for DID, private TIE, or outgoing public calls. This consolidation means that it may be possible for each office to use a single PRI span, rather than two T1 spans. With PRI Call-by-Call services, the only limitation is that there are no more than 23 calls in progress at any one time.

The dialing plan at each BCM site is configured to determine the call type based on the digits dialed by the user. If a user in Toronto wishes to dial a colleague in New York, they dial the four-digit private DN (such as 6221). The dialing plan recognizes this as a private network DN, and routes the call using TIE service with a private dialing plan.

Incoming TIE calls are routed to telephones based on the digits received by the network, which in this case is the four-digit private DN.

If a user in either location wishes to dial an external number, they dial 9, followed by the number (such as 9-555-1212). The dialing plan recognizes this as a public DN, and routes the call using Public service.

Incoming DID calls are routed to telephones, based on the trailing portion of the digits received by the network. For example, if a public network user dials an employee in the Toronto office, the network delivers digits 4167632221. The BCM routes the call using the last four digits, 2221, to the BCM450.

Refer to the following table for a description of the settings required for this type of routing service.

Table 35 PRI Call-by-Call services routing information

Parameter		Home System Settings	
Hardware			
	DTM	PRI	
	Protocol	NI-2	
Trunk/Line Data			
	Line 125	Target line	
	Private/Public Received #	2221	
Line Access			
	DN 2221	L125:Ring only	
	Line pool access	Line pool BlocA	
Routing Services		Private Network	Public network
		New York:	Public network
Route		001	002
External #		No number	No number
Use		Pool BlocA	Pool BlocA
Service type		TIE	Public
ServiceID		1	N/A
DN type		Private	N/A
Destination Code		6	9
Normal route		001	002
Absorb		0	ALL
New York office:			
Parameter		Home System Settings	
Hardware			
	DTM	PRI	
	Protocol	NI-2	
Trunk/Line Data			
	Line 125	Target line	
	Private/Public Received #	6221	
Line Access			
	DN 6221	L125:Ring only	
	Line pool access	Line pool BlocA	

Table 35 PRI Call-by-Call services routing information

Parameter	Home System Settings	
	Private Network	Public Network
Routing Services	Toronto	Public Network
Route	001	002
External #	No number	No number
Use	Pool BlocA	Pool BlocA
ServiceType	TIE	Public
ServiceID	1	N/A
DN type	Private	N/A
Destination Code	2	9
Normal route	001	002
Absorb	0	ALL

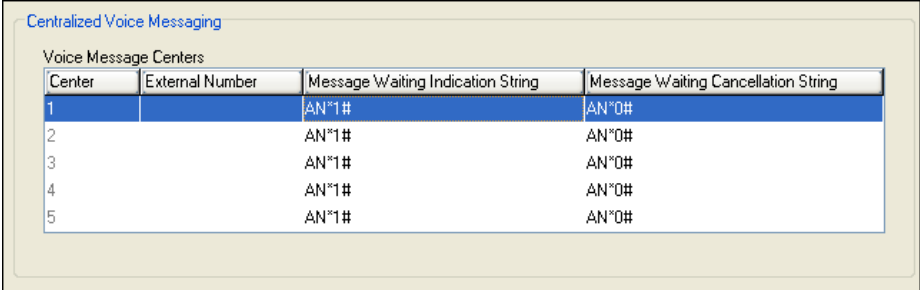
Voice messaging

This section gives an overview of voice messaging service. You can have either an internal voice message service, or you can connect your system to an external voice message service, either over the PSTN network to a message center at the central office or through a private network to another system.

Centralized voice messaging (ext mail)

This panel allows you to record on the system the dial strings that allow users on your system to access a remote voice messaging service. Note that public or private trunks need to be properly configured for these numbers to work. To access the Voice Message Centers table, click Configuration > Applications > Voice Messaging/Contact Center.

Figure 34 Voice Message Centers table



The screenshot shows a web interface titled "Centralized Voice Messaging". Inside, there is a section labeled "Voice Message Centers" containing a table with four columns: "Center", "External Number", "Message Waiting Indication String", and "Message Waiting Cancellation String". The table has five rows, with the first row highlighted in blue.

Center	External Number	Message Waiting Indication String	Message Waiting Cancellation String
1		AN*1#	AN*0#
2		AN*1#	AN*0#
3		AN*1#	AN*0#
4		AN*1#	AN*0#
5		AN*1#	AN*0#

The following table describes each field on this panel

Table 36 Voice Message Centers Table

Attribute	Values	Description
Center	<read-only>	You can define a maximum of five external voice message centers. Note that any one user can only be connected to one center.
External Number	<dial string>	This is the number for the external voice message center. Ensure that you add the appropriate routing information.
Message waiting indication (MWI) string	<string>	Indicates that the message center has a message in the mailbox. This is a default NSI string for message waiting. Refer to MWI and MWC strings programming (page 156)
Message wait cancellation string (MWC)	<string>	Indicates that the voice messages have been retrieved. This is a default NSI string for message waiting.

MWI and MWC strings programming

MWI and MWC information is received from the network in the form of NSI strings.

The default MWI and MWC strings are default NSI strings for Message Waiting.

*58B*AN*1# – Message Waiting Indication

*58B*AN*0# – Message Waiting Cancellation

This provides the information required to program the strings as:

AN*1# for MWI, and AN*0# for MWC Private network strings differ with different message centers. These should only be changed on the advice of your customer service representative.

DPNSS: The NSI strings in DPNSS are dependent on the supplier of the PBX. Therefore, the strings vary depending on the originating PBX system. Each string has the following default structure: *58XXXXXX.*

The following table describes each part of the NSI string.

Table 37 Parts of the NSI string

String Component	Description
*58	Identifies that it is an NSI string.
X	Any letter from A to Z, or nothing.
YYYYY..	Manufacturer specific string, which can contain any sequence of alphanumeric digits or *.
#	Marks the end of the identifier.

Only the YYYYY.. # portion of the string must be programmed for MWI and MWC. The procedure is similar to Set Name/Line Name.

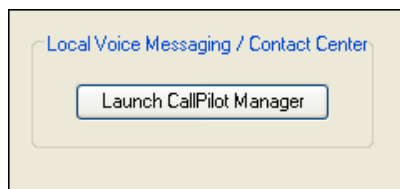
The following criteria must be met when programming NSI strings for MWI/MWC:

- No spaces are allowed, including spaces at the end of the string.
- A # must be present at the end.
- A # or a * cannot be present in the first character.

Local vox msg access (CallPilot)

Local voice messaging is configured using a client application. This CallPilot application is explained in detail in the CallPilot documentation.

Click the Launch CallPilot Manager button to access the application from which you can set up your local voice messaging system.



Silent record-a-call network storage locations

To access the Silent Record-a-Call Network Storage Locations panel, select **Configuration > Voice Messaging / Contact Center**.

The administrator can configure up to 10 network SFTP servers to store WAV files recorded from the Record a Call feature. The administrator can then configure the COS feature setting, Record Call SFTP Dest, with a number that corresponds to one of the SFTP locations in the table.

Centralized voice mail

This section gives an overview of centralized voice mail.

Refer to the following information:

- [Voicemail with local system as host \(page 159\)](#)
- [Voicemail with Meridian 1 as host \(page 159\)](#)
- [System-level setup for voicemail \(page 160\)](#)
- [Satellite impacts on VoIP networking \(page 161\)](#)
- [Configuration levels \(page 160\)](#)

Voicemail with local system as host

A local system that acts as a central voice-mail location must be able to support MCDN. You can add up to 1000 mailboxes on BCM voice mail, providing you have entered adequate keycodes.

Voicemail with Meridian 1 as host

If you are using a voice mail system connected to a Meridian 1 as a host system, ensure that the systems are set up to be compatible with each other.

DMS-100/SL100 inter-op for voicemail

DMS-100/SL100 centralized voice mail: The BCM can also support centralized voice mail on a DMS-100/SL100 switch through a PRI-DMS-100 connection. The system also supports centralized voice mail on the switch through an indirect connection through an M1, where the DMS-100/SL100 is connected by PRI-DMS-100 to the M1, and the M1 is connected to a BCM through a PRI-MCDN connection. The DMS-100/SL100 can use either the Public number or Private number of a BCM telephone to designate the mailbox number on the voice mail system.

Prerequisites for configuring voicemail

To configure centralized voice mail, the system must be using a CDP dialing plan and be running on a private network created using either DPNSS (UK profile), PRI SL-1 or VoIP trunking set up with MCDN. Private network configuration and features are discussed in [Private networking—MCDN over PRI and VoIP \(page 111\)](#).

Attention: For centralized voice mail from a BCM system, configure the BCM dialing plan as either CDP or UDP.

CallPilot constraints

For details about setting up the CallPilot parameters and features, refer to the CallPilot Manager Set Up and Operations Guide and the other CallPilot supporting documentation.

- To allow use of the auto attendant feature, you must ensure that the Allow Network Transfers check box is selected in the CallPilot Manager.
- To allow use of voice mail, you must ensure that the Enabled Redirected DN check box is selected in the CallPilot Manager.
- A target line must be set up to be answered by the auto attendant. The target line received digits should match the voice mail DN.

Configuration levels

The BCM supports voice-mail configuration either from the local source or by accessing a remote voice mail system located on another BCM, located on a BCM450, or attached to a Meridian 1 system. The system can be configured to more than one voice mail system. However, each telephone can only be configured to one system.

System-level setup for voicemail

The system that hosts the voice mail needs to ensure that incoming calls are directed to the voice mail service.

Process assumptions:

- Private network is set up, with MCDN, between any nodes that need to access voice mail on this system.
- All systems are using the CDP dialing plan, and you have set up the correct routing to these systems.
- CallPilot or auto attendant is set up and is running for the local system.
- You have obtained a list of DNs from the remote systems that require mailboxes.

Host impacts on VoIP networking

If you are using H.323 VoIP trunks for central voice mail, you need to set the following:

- Ensure that the local gateway protocol is set to SL-1 or CSE, based on the version of the satellite systems.
- Ensure that the remote gateways are programmed to route using CDP.
- Ensure that the remote gateway protocols are set to SL-1 or CSE, based on the version of the satellite system.

Satellite impacts on VoIP networking

Systems that are remote to the voice mail system need to ensure that outgoing calls are correctly directed to the voice mail service on the host system.

Process assumptions:

- Private network has been set up, with MCDN, between the satellite and host system.
- The correct routing to the host system is set up and working.
- You have supplied a list of DNS to the host system administrator that require mailboxes.

VoIP overview

This section gives an overview of VoIP.

Uses for VoIP

On the BCM, the LAN configuration consists of Main Module LAN configuration, which determines how the Main Module of the BCM communicates with other devices on the LAN.

Prerequisites for VoIP

Answer the questions in the following table if you are configuring VoIP trunks.

Table 38 VoIP trunk provisioning

Prerequisites	Yes	No
Have you confirmed the remote gateway settings and access codes required?		
Have you determined the preferred codecs required for each type of trunk and destination?		
Have you set up line parameters, determined line pools for H.323 trunks, and set up destination codes? Have you determined which system telephones will have access to these routes?		
If you have not already assigned target lines, have you defined how you are going to distribute them on your system?		
Have you decided if you are going to employ the fallback feature? If yes, ensure that your routing and scheduling are set up. Ensure that QoS is activated. If either of these conditions is not met, your H.323 trunks will not work correctly.		

Key VoIP traffic concepts

The following explains a few commonly used VoIP terms.

QoS

QoS (Quality of Service) is technology that determines the maximum acceptable amount of latency, and balances that with the quality of the VoIP connection. BCM and network routers use QoS to ensure that real time critical IP packets, such as voice packets, are given higher routing and handling priority than other types of data packets.

Silence suppression

Silence suppression technology identifies the periods of silence in a conversation, and stops sending IP speech packets during those periods. Telco studies show that in a typical telephone conversation, only about 36% to 40% of a full-duplex conversation is active. When one party in the conversation is quiet for more than a few hundredths of a second, voice packet transmission is suppressed until the party starts talking again. This is half-duplex. There are important periods of silence during speaker pauses between words and phrases. By applying silence suppression, average bandwidth use is reduced by the same amount. This reduction in average bandwidth requirements develops over a 20-to-30-second period as the conversation switches from one direction to another.

Codecs

The algorithm used to compress and decompress voice over IP networks and VoIP trunks is embedded in a software entity called a codec (COde-DECcode).

- The G.711 Codec samples the voice stream at a rate of 64 kbps (kilo bits per second), and is the Codec to use for maximum voice quality. Choose the G.711 Codec with the companding law (alaw or ulaw) that matches your system requirements.
- The G.729 Codec samples the voice stream at 8 kbps. The voice quality is slightly lower using a G.729 but it reduces network traffic by approximately 80%.
- The G.723 Codec should be used only with third party devices that do not support G.729 or G.711.

Codecs with Silence Suppression, also referred to as VAD (Voice Activity Detection), make VAD active on the system, which performs the same function as having silence suppression active.

Proactive voice quality management

Proactive Voice Quality Monitoring (PVQM) provides real-time notification in case of voice over IP call quality degradation, thus allowing you to monitor and manage calls on the network in real time. As a result, you can be aware of, and respond to, changing network conditions in a proactive way.

PVQM monitors a set of metrics which include

- packet loss
- inter arrival jitter
- round trip delay
- Listening R

These metrics and supplementary information provide you with valuable insight into the real time quality of the call from the end-user perspective. This information gives an indication of the type of problem, and can be used to locate the source of the issue, thus accelerating the isolation and diagnostics phase of problem resolution.

In addition to packet loss, inter arrival jitter and round trip delay, PVQM monitors the “listening R” value. The R-Factor, as defined by ITU G.107 and IETF 3611, is a call quality index that assesses network impairments such as packet drops, jitter and round trip delay with consideration for the burstiness and recency of these impairments. The Listening R metric provides you with definitive answers about the actual QoS delivered to the telephone user. With this metric, you see the raw data (such as jitter or packet drop rate), and a summary of the effect of the data on the quality experienced by the user.

For example, a Warning Threshold for the listening R-value might be set at 80. When voice quality drops below this value as measured at the telephone set itself, an event is generated. The event notification is augmented with other valuable state information, such as network loss rate, average rate of discards due to jitter, average length of bursts, and presented as an alarm. Analysis of the alarms and supplementary information in the alarm description helps you identify and troubleshoot voice quality issues and proactively initiate responsive actions.

Refer to *Nortel Business Communications Manager 450 1.0 Administration and Security* (NN40160-601) for information on how to configure and use PVQM functionality.

IP telephones in VoIP network

IP telephones offer the functionality of regular telephones but do not require a hardwire connection to the BCM. Instead, they must be plugged into an IP network, which is connected to the LAN or WAN on the BCM. Calls made from IP telephones through the BCM can pass over VoIP trunks or across a Public Switched Telephone Network (PSTN).

Nortel has several types of IP telephones that connect to the BCM through Ethernet. The IP softphone 2050, which runs as a client application on a PC or PDA, also connects to the BCM through the Ethernet.

VoIP trunks

VoIP trunks allow voice signals to travel across IP networks. A gateway within the BCM converts the voice signal into IP packets, which are then transmitted through the IP network to a gateway on the remote system. The device at the other end reassembles the packets into a voice signal.

IP telephony and programming

The BCM can communicate using digital telephones (7000, 7100, 7100N, T7208, 7208, 7208N, 7316, 7316E, 7316E+KIMs, and 7310), cordless telephones (7406, 7406E), and IP telephones and applications (Nortel IP Phone 2001, IP Phone 2002, IP Phone 2004, Nortel IP Softphone 2050, IP Phone 2007, IP Phone 1110, IP Phone 1120e, IP Phone 1140e, IP Phone 1210, IP Phone 1220, and IP Phone 1230, WLAN Handset 2210, WLAN Handset 2211, WLAN Handset 2212, WLAN Handset 6120, and WLAN Handset 6140). With this much flexibility, the BCM can provide the type of service you require to be most productive in your business.

Attention: Model 7000 phones are supported in selected markets only.

While analog and digital telephones cannot be connected to the BCM system using an IP connection, they can make and receive calls to and from other systems through VoIP trunks. Calls received through the VoIP trunks, or other IP telephones, to system telephones are received through the LAN or WAN card and are translated within the BCM to voice channels.

Gatekeepers

A gatekeeper tracks IP addresses of specified devices, and provides routing and (optionally) authorization for making and accepting calls for those devices. A gatekeeper is not required as part of the network to which your BCM system is attached, but gatekeepers can be useful on networks with a large number of devices.

When planning your network, be sure to consider all requirements for a data network. Consult your network administrator for information about network setup and how the BCM fits into the network.

SIP proxy

A SIP Entity that receives requests and sends them on to another proxy or to their final destination. A Proxy uses the information retrieved from the Location Service in order to find an alias or an actual destination address for the request. Alternatively, a Proxy can be statically configured, in which case registration is not necessary.

IP LANs and WANs

A Wide Area Network (WAN) is a communications network that covers a wide geographic area, such as state or country. For CallPilot, a WAN is any IP network connected to a WAN card on the CallPilot system. This can also be a direct connection to another CallPilot system.

If you want to deploy IP telephones that will be connected to a LAN outside of the LAN that the BCM is installed on, you must ensure the BCM has a WAN connection. This includes ensuring that you obtain IP addresses and routing information that allows the remote telephones to find the BCM, and vice versa.

A Local Area Network (LAN) is a communications network that serves users within a confined geographical area. For BCM, a LAN is any IP network connected on the BCM system. Often, the LAN can include a router that forms a connection to the Internet. A BCM can have up to two LAN connections.

VoIP trunk gateway configuration

This section describes how to configure VoIP trunk gateway.

DTMF handling using RFC2833

RFC2833 is an in-band mechanism for DTMF signaling. This feature enables the BCM SIP gateway to send and receive DTMF using RFC2833.

RFC2833 is the only mechanism for reliable DTMF signaling in SIP. No standard out-of-band signaling exists. Traditional in-band signaling (DTMF as a voice) is reliable for G.711 only.

Some limitations and restrictions to this feature apply:

- The BCM does not support RFC2833 over H.323 trunks.
- IP phones do not support long tones.
- Long tones feature is not supported on H.323 trunks.
- RFC2833 long tones received from the network are converted into short tones.
- IP phones do not support RFC2833 detection.
- SIP trunks do not support military tones A, B, C, and D.
- The BCM supports a subset of RFC2833 tones and signals, specifically DTMF signals for 9, *, and #.
- The BCM accepts all three signaling methods (RFC2833, Out Of Band, DTMF as tone) from SIP endpoints. The sender must choose only one method for DTMF signaling to prevent digit duplication.

The following path indicates where to set up DTMF handling using RFC2833 in Element Manager:

- Element Manager: **Configuration > Resources > Telephony Resources**. Select an IP Trunk and click on the SIP Settings tab

SIP proxy configuration

The SIP Proxy panel has two subpanels: SIP Proxy and Outbound Proxy. Together these settings form the SIP Proxy configuration for the BCM.

The SIP Proxy subpanel provides the data used in SIP message headers and provides the actual SIP Proxy server used to route SIP calls.

On the Outbound Proxy subpanel, you can configure a group of outbound proxy servers that provide proxy failover services.

With SIP proxy failover, the BCM has a group of SIP proxy servers that provide load balancing of proxy use and detection of non responsive proxies. Each proxy is given a weight. An outgoing call is directed to one of the proxy servers in the group, according to its weight.

A setting on the SIP Proxy tab, Route all calls using proxy, determines whether the BCM routes calls using the routing table or the SIP proxy configuration. If you select this check box, the BCM bypasses the routing table and uses the SIP proxy configuration to route calls.

The following path indicates where to set up SIP proxy in Element Manager:
Element Manager: **Configuration > Resources > Telephony Resources**.

Configuration for SIP authentication

With SIP authentication, the BCM can

- challenge incoming calls to ensure callers are authorized to place calls to the local system
- authenticate itself to remote servers that request authentication

SIP calls are not authenticated based on individual calls. If SIP authentication is on, the system authenticates all SIP calls. If SIP authentication is off, the system does not authenticate SIP calls.

The BCM handles SIP authentication on a request-by-request basis with a challenge–response mechanism based on user name and password combinations. The BCM stores these user name and password combinations in tables on the BCM. There is one table for incoming calls and one for outgoing calls.

If you enable Local Authentication, the BCM challenges an incoming call. The remote domain answers with an authentication reply that contains the configured user name and password for the local system. The user name and password combination must match an account in the Local Accounts table.

If a remote domain challenges an outgoing call from the BCM, the BCM answers with an authentication reply that contains the configured user name and password for the remote domain. If the BCM is not configured for the remote domain, the BCM attempts authentication with an anonymous user name and empty password combination.

The following path indicates where to set up SIP authentication in Element Manager: Element Manager: **Configuration > Resources > Telephony Resources**. Select an IP Trunk and click the Sip Proxy tab.

VoIP trunk gateways

This section provides an overview of VoIP trunk gateways.

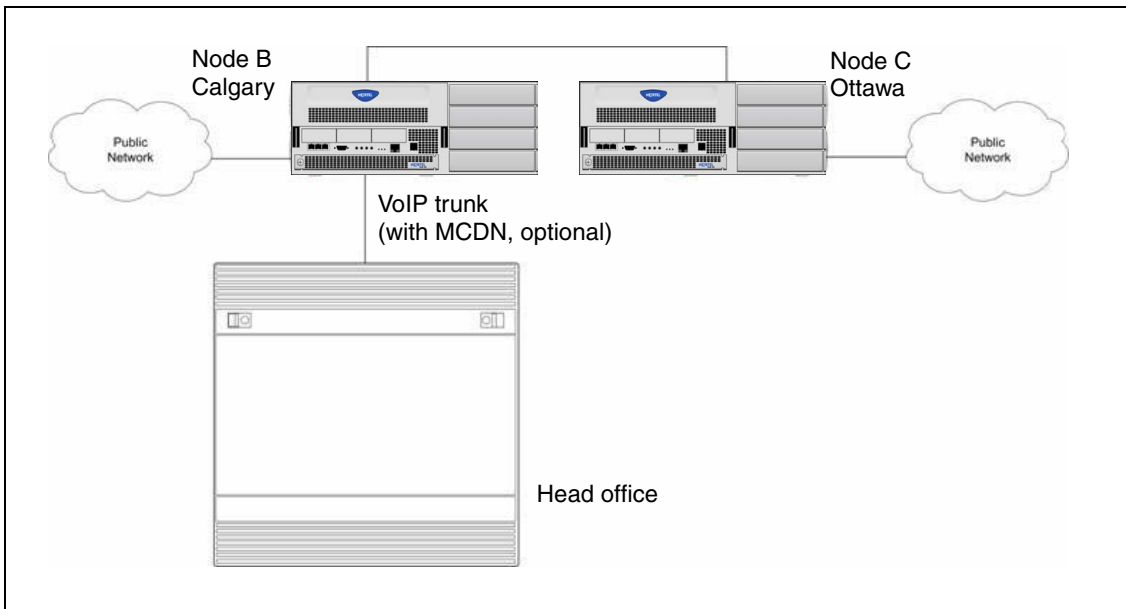
Uses for VoIP trunk gateways

You can use a VoIP trunk to establish communications between a BCM and a remote system across an IP network. Each trunk is associated with a line record (lines 001-130), and are configured in the same way that other lines are configured.

You can use VoIP trunks for calls originating from any type of telephone within the BCM system. Calls coming into the system over VoIP trunks from other systems can be directed to any type of telephone within the system.

How VoIP trunks make a network

The following figure shows a simple private networking configuration of three systems connected by VoIP trunks. As in all private networking, each system has direct routing configurations to the directly adjacent systems. As well, the dialing plans are configured to ensure that remote calls are correctly routed to the receiving system, such as, if Node A called someone in Node C.

Figure 35 Internal call from Meridian 1 tandems to remote PSTN line

Since the VoIP trunks are configured into line pools, you can assign line pool codes to users who have been assigned access to the VoIP trunks. However, if you intend to set up your system to use fallback, so that calls can go out over PSTN if the VoIP trunks are not available, you must use routes and destination codes to access the VoIP trunk line pools.

Prerequisites for VoIP trunk gateway configuration

Ensure that you have obtained the following information or familiarize yourself with the requirements before continuing with VoIP trunk configuration:

- Keycodes:** Obtain and install the necessary keycodes for the number of VoIP trunks you want to support on the system. See the *Keycode Installation Guide* (NN40010-301) for more information about installing the keycodes. Talk to your BCM sales agent if you need to purchase VoIP keycodes.
 Each keycode adds a specific number of VoIP trunks. You must reboot your BCM after you enter VoIP keycodes to activate trunking.
 FEPS (Functional Endpoint Proxy Server), the VoIP Gateway service, restarts automatically after you enter the VoIP keycodes.
- H.323 network applications considerations**
 If your network uses a gatekeeper (H.323 trunks only), specific settings are available to configure on your system to recognize the gatekeeper. Additional settings are available within the gatekeeper application to configure VoIP lines. See [VoIP interoperability—gatekeeper configuration \(page 189\)](#). If a gatekeeper exists on the network, you need not configure remote gateway settings. For audio stream ports, see [Scope of optional VoIP trunk configurations \(page 181\)](#)

If you plan to use H.323 trunking and you have a firewall, ensure that the ports you intend to use are allowed. H.323 uses ports 1718, 1719, and 1720.

- SIP network applications consideration
If you plan to use SIP trunking and you have a firewall, ensure that the ports you use are allowed. SIP uses port 5060. For audio stream ports, see [Scope of optional VoIP trunk configurations \(page 181\)](#).

VoIP trunk gateway keycodes

Before you can use VoIP, you must obtain and install the necessary keycodes. Talk to your BCM sales agent if you need to purchase VoIP keycodes.

Each keycode adds a specific number of VoIP trunks. To activate trunking, you must reboot your BCM after you enter VoIP keycodes. If you want to use the MCDN features on the VoIP trunks, you must have an MCDN keycode. If you have already deployed MCDN for your SL-1 PRI lines, you do not require an additional keycode.

H.323 network applications considerations

In order to maintain a level of quality during call setup, QoS monitor must be enabled and configured.

If your network uses a gatekeeper (H.323 trunks only), there are also specific settings that must be set on the H323 Settings panel to recognize the gatekeeper, and also within the gatekeeper application, so that VoIP lines are recognized. Also refer to gatekeeper configuration [VoIP interoperability—gatekeeper configuration \(page 189\)](#).

If you plan to use H.323 trunking and you have a firewall set up, ensure that the ports you intend to use have been allowed.

SIP network application considerations

In order to maintain a level of quality during call setup, QoS monitor must be enabled and configured.

SIP URI maps of both endpoints must match.

If you plan to use SIP trunking and you have a firewall set up, ensure that the ports you intend to use have been allowed.

Local gateway programming

The VoIP trunk access point at each system is called a gateway. The gateway to your system, the local gateway, determines how incoming and outgoing calls are handled.

The H323 and SIP Media Parameters tabs determine a number of system settings. These values need to be coordinated with the other systems on the network to ensure that all features work consistently across the network. Media parameters include setting:

- the order of preferred codecs
- voice activity detection
- jitter buffer size
- codec payload size
- IP fax transmission availability on the network

The local gateway parameters define how the BCM prefers call signaling information to be directed through VoIP trunks. Call signaling establishes and disconnects a call.

If the network has a gatekeeper (H.323 trunks only), the BCM can request a method for call signaling, but whether this request is granted depends on the configuration of the gatekeeper. Ultimately, the gatekeeper decides which call signaling method to use.

Local gateway settings include

- fallback to circuit switched availability and scope
- type of call signaling, either directly to the far end system or through a network gatekeeper
- if there is a gatekeeper, the relevant IP information is noted
- a KeepAlive signal timer
- the protocol the system uses for the gateway (must be compatible with remote system or gatekeeper)
- allowing/disallowing VoIP gateway tunnel H.245 messages within H.225
- being able to identify unique call signaling and RAS ports

Notes about NPI-TON aliases for H.323 trunks

NPI-TON aliases store dialed number prefixes as well as information about the type of number. A dialed number can be qualified according to its TON (type of number), as well as its NPI (numbering plan identification). Nortel recommends this format over the E.164 format, for encoding dialed numbers and aliases registered with a gatekeeper.

When using a gatekeeper, and attempting to place an outgoing VoIP trunk call, ensure that the route and dialing plan configuration matches the NPI-TON aliases registered, by the destination, with the gatekeeper. These requirements are summarized in the following table.

Table 39 Route and Dialing Plan configurations for NPI-TON

Route (DN type)	Dialing Plan used by calling gateway	Alias configured for calling gateway ("alias name" in Element Manager)
Public	Public	PUB:<dialDigitsPrefix>
Private	Private (Type = None)	PRI:<dialDigitsPrefix>
	Private (Type = CDP)	CDP:<dialDigitsPrefix>
	Private (Type = UDP)	UDP:<dialDigitsPrefix>

VoIP routing table

Since VoIP trunks are point-to-point channels, besides the local gateway information on your system, you need to tell your system about the gateway at the remote end.

However, if the network has a gatekeeper or a SIP Proxy Server, it handles call traffic, so a routing table is not required.

To configure a remote gateway, you need to define the following information:

- a name that identifies the destination system
- the IP address of the destination system
- the IP address of the destination system
- transmit threshold so that the system knows when to activate the fallback feature
- the remote gateway system type
- the gateway protocol
- the unique digit(s) that identify the remote system. (this is usually part of the destination code)

PSTN access to a remote node

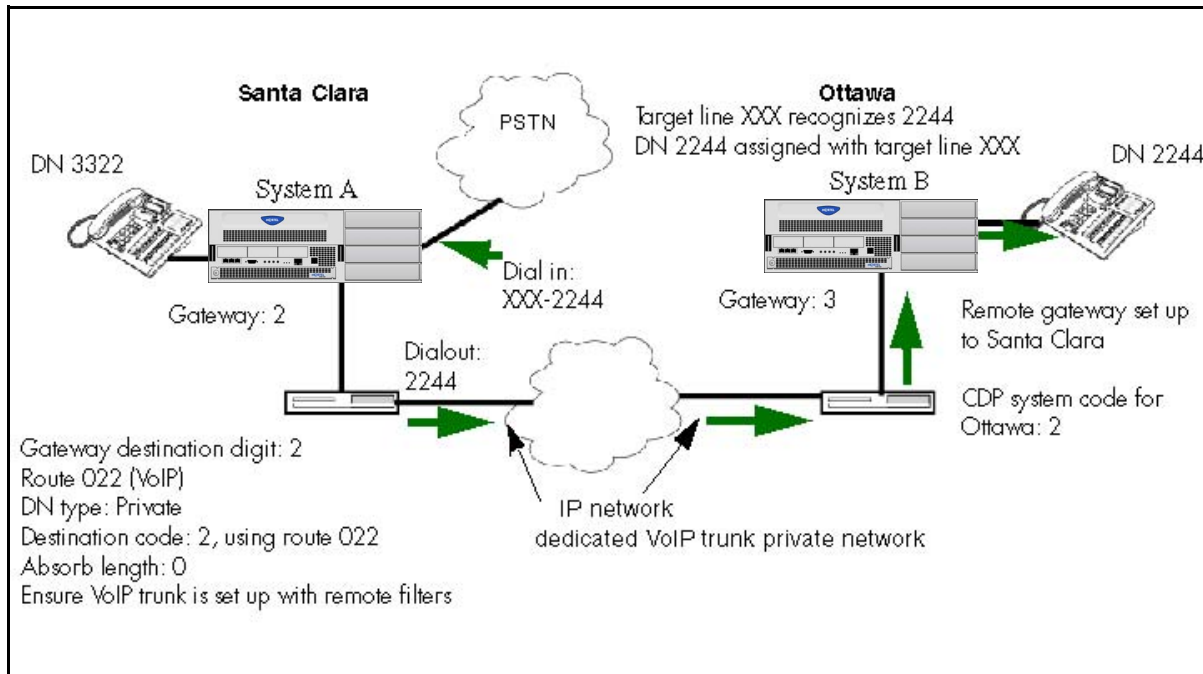
Making a call to a remote node requires any BCM systems between the calling and receiving nodes to have the correct routing to pass the call on to the next node. This is the same if you use PSTN lines or VoIP trunks for the network.

The following figure shows a call tandeming from the public network (PSTN), through System A (Santa Clara) and being passed to System B (Ottawa) over a VoIP trunk network. In this case, it might be a home-based employee who wants to call someone in Ottawa.

You cannot program DISA for VoIP trunks, therefore, your system cannot be accessed from an external location over a VoIP trunk. The exception to this is if the call comes into a tandemed system (system A) from a PSTN, and the call is then sent out across a VoIP trunk to system B, as in this example. In this

case, system A is controlling remote access through remote access packages and routing, transferring the outside call to a VoIP trunk, which is accessed by an allowed dial sequence. The VoIP trunk connects directly to system B, where the dialing sequence is recognized as directed to an internal DN. In this scenario, all remote call features are available to the caller.

Figure 36 Calling into a remote node from a public location



Fallback to PSTN from VoIP trunks

Fallback is a feature that allows a call to progress when a VoIP trunk is unavailable or is not providing adequate quality of service (QoS).

Refer to the information under [Fallback to PSTN from VoIP trunks \(page 178\)](#) for details about setting up fallback for VoIP trunks.

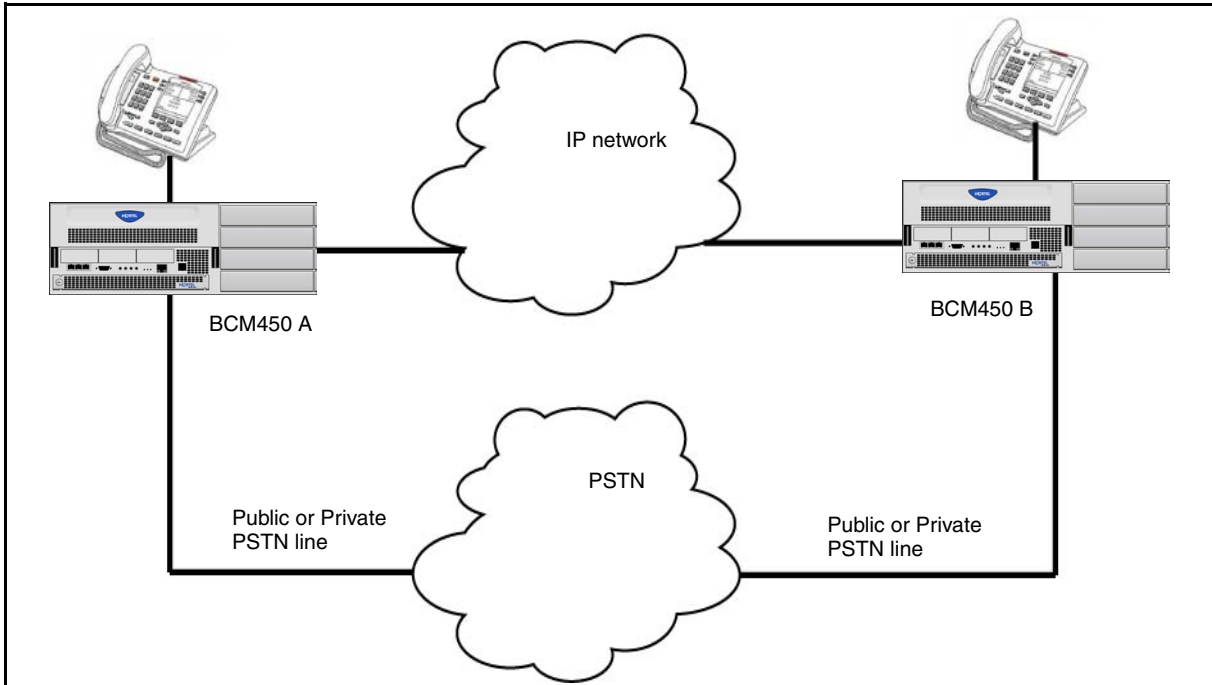
By enabling Fallback to circuit-switched on the H323 Settings or SIP Settings panels, you allow the system to check the availability of a VoIP trunk, then switch the call to a PSTN line, if the VoIP trunk is not available. For the to work on a suitable bandwidth, QoS monitor must be enabled and a transmit threshold must be set. For QoS and transmit threshold settings refer to the following table.

Use the dialing plan worksheet in the Programming Records to plan your dialing requirements so you can pinpoint any dialing issues before you start programming. If you are programming an existing system, you can look at what numbers the users are familiar with dialing, and you can attempt to accommodate this familiarity into your destination codes plan.

On any IP gateway for which you want to allow fallback based on network quality, you need to ensure that QoS monitor is enabled.

The following figure shows how a fallback network would be set up between two sites.

Figure 37 PSTN fallback diagram

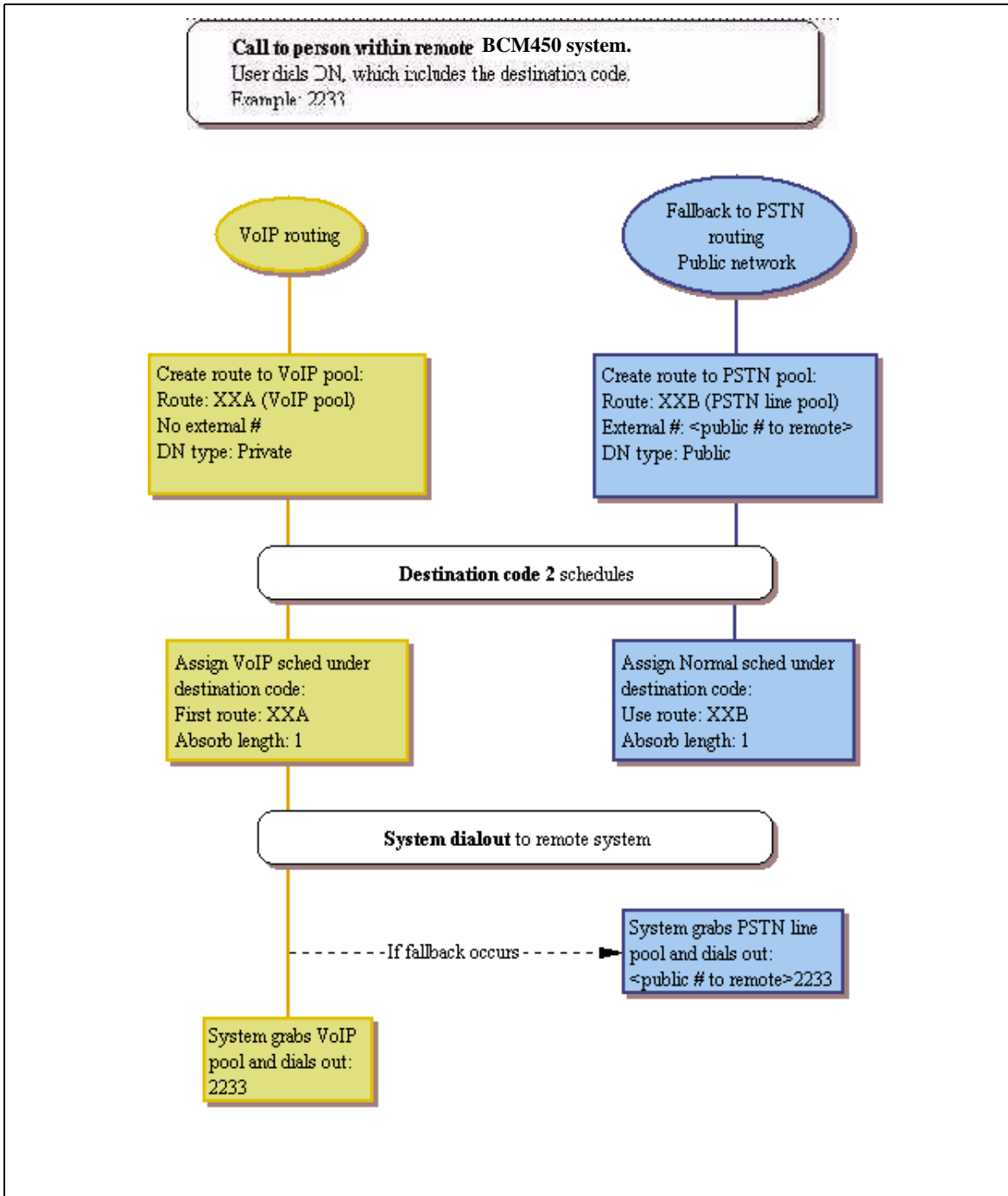


Fallback routing, UDP networks

The user dials 2233 (remote system DN: 2233; destination digits/private access code: 555). The system then adds the private access code to the dialout digits. If the call falls back to PSTN line, the system then dials out the private access code (private network PSTN line) or public access number (public PSTN) to the remote system in front of the 2233.

Fallback routing, CDP networks

User dials 2233 (remote system DN: 2233; remote identifier/destination digit: 2). The system absorbs the 8, no other digits are absorbed and the system dials out 2233. If the call falls back to PSTN line, the system still only absorbs the 8. If the PSTN line is on a private network, the system dials out 2233. If the PSTN line is a public line, the system dials out the public access number to the remote system in front of the 2233. See the following figure.

Figure 38 Setting up routes and fallback for call to remote system (CDP dialing code)


Scope of optional VoIP trunk configurations

A number of VoIP trunk features are optional to setting VoIP trunk functions. The following briefly describes these features:

- Port settings (firewall): In some installations, you may need to adjust the port settings before the BCM can work with other devices. Firewalls can interfere with communications between the BCM and another device. The port settings must be properly configured for VoIP communications to function properly. Using the instructions provided with your firewall, ensure that communications using the ports specified for VoIP are allowed.

A Nortel IP telephone uses ports between 51000 and 51200 to communicate with the system. The system, by default, uses ports 28000 to 28255 to transmit VoIP packets.

BCM uses UDP port ranges to provide high priority to VoIP packets in existing legacy IP networks. You must reserve these same port ranges and set them to high priority on all routers that an administrator expects to have QoS support. You do not need to reserve port ranges on DiffServ networks.

You can select any port ranges that are not used by well-known protocols or applications.

Each H.323 or VoIP Realtime Transfer Protocol (RTP) flow uses two ports, one for each direction. The total number of UDP port numbers to be reserved depends on how many concurrent RTP flows are expected to cross a router interface. In general:

Include port number UDP 5000 in the reserved port ranges, for the QoS monitor.

The port ranges reserved in a BCM system are also reserved by the remote router.

You must reserve two ports for each voice call you expect to carry over the IP network.

You can reserve multiple discontinuous ranges. BCM requires that each range meet the following conditions: Each range must start with an even number; each range must end with an odd number; no more than 256 ports can be reserved.

Attention: By default SIP uses port 5060.

- Gatekeepers: The BCM supports the use of an ITU-H323 gatekeeper. A gatekeeper is a third-party software application residing somewhere on the network, which provides services such as:
 - address translation
 - call control
 - admission control
 - bandwidth control
 - zone management
 - IP registration

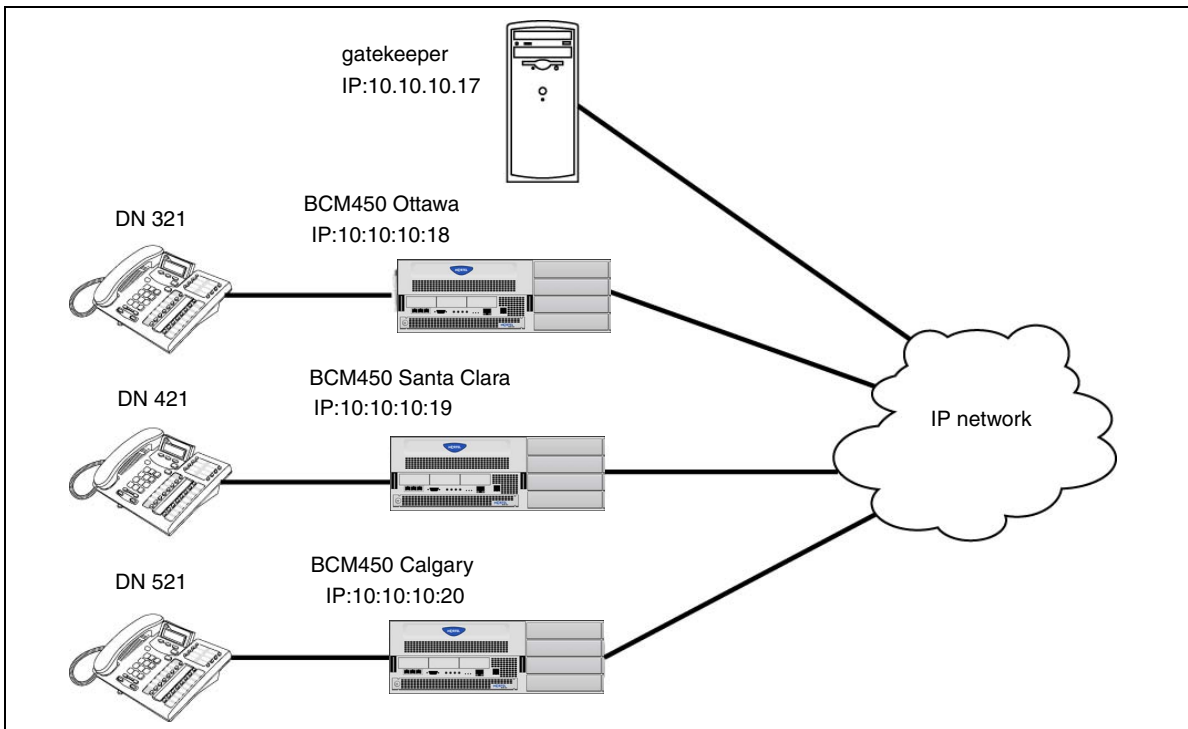
A single gatekeeper manages a set of H.323 endpoints. This unit is called a Gatekeeper Zone. A zone is a logical relation that can unite components from different networks (LANS). These Gateway zones, such as the BCM, are configured with one or more alias names that are registered with the gatekeeper. The gatekeeper stores the alias-IP mapping internally and uses them to provide aliases to IP address translation services. Later, if an endpoint IP address changes, that endpoint must re-register with the gatekeeper. The endpoint must also re-register with the gatekeeper during the time to live (TTL) period, if one is specified by the gatekeeper.

Refer to the gatekeeper software documentation for information about changing IP addresses.

Attention: A gatekeeper can help to simplify IP configuration or the BCM dialing plan; however, it does not simplify the network dialing plan.

Gatekeeper call scenarios

The following explains how a call would be processed for the two types of gatekeeper configurations. The following figure shows a network with three BCMs and a gatekeeper.

Figure 39 BCM systems with a gatekeeper

This example explains how a call from DN 321 in Ottawa would be made to DN 421 in Santa Clara. It assumes that call signaling is set to Gatekeeper Resolved and no pre-granted AdmissionRequest (ARQ) has been issued:

- 1 BCM Ottawa sends an ARQ to the gatekeeper for DN 421.
- 2 The gatekeeper resolves DN 421 to 10.10.10.17.
- 3 BCM Ottawa sends the call Setup message for DN 421 to the gatekeeper (10.10.10.17), which forwards it to the gateway at 10.10.10.19.
- 4 The call is established.

Faxing over VoIP trunks: You can assign VoIP trunks to wired fax machines if you have T.38 fax enabled on the local gateway. The BCM supports this IP fax feature between BCMs, BCM200/400/1000 running BCM 3.5 and subsequent up-level versions of software, and a Meridian 1 running IPT 3.0 (or newer) software, or a CS 1000/M.

The system processes fax signals by initiating a voice call over the VoIP line. When the T.38 fax packets are received at the remote gateway, the receiving system establishes a new path that uses the T.38 protocol. Both the endpoints must be running a software version that supports the T.38 fax.

**CAUTION Operations note:**

Fax tones that broadcast through a telephone speaker can disrupt calls at other telephones using VoIP trunks in the vicinity of the fax machine. Here are some suggestions to minimize the possibility of your VoIP calls being dropped because of fax tone interference: Locate fax machine away from other telephones.

Turn the speaker volume on the fax machine to the lowest level, or off.

Fax tones recorded in a voice mailbox: In the rare event that fax tones are captured in a voice mail message, opening that message from an telephone using a VoIP trunk causes the connection to fail.

For a list of limitations and requirements for using T.38 fax, refer to [Operational notes and restrictions \(page 184\)](#).

Operational notes and restrictions

Some fax machines are unable to successfully send faxes over VoIP (T.38) trunks to the following destinations:

- CallPilot mailboxes
- CallPilot mailboxes (accessed through auto-attendant)
- Fax Transfer (calls transferred to a system fax device through the auto-attendant)

Use the following tips to avoid this problem:

- Avoid the use of manual dial on the originating fax machine. In some fax machines, manually dialing introduces a much shorter call time-out.
- If manual dial must be used, then the user should wait until the call is answered before starting the fax session.
- If manual dial must be used, then the user should enter the digit 8 before initiating the fax session. This ensures that the fax session is initiated by CallPilot before the fax machine's timer is started.
- The call duration can be increased by adding a timed pause to the end of dialing string (for example: 758-5428,,,). This allows the call to ring at the destination before the fax machine call duration timer starts.
- Since the problem is related to the delay in initiating the fax session, the number of rings for fax mailboxes Call Forward No Answer (CFNA) should be minimized.

The following table is a list of restrictions and requirements for the T.38 fax protocol.

Table 40 T.38 restrictions and requirements

Supported	Not supported
only UDP transport	TCP
only UDP redundancy	Forward Error Correction (FEC)
T.38 version 0	Fill removal
on H.323 VoIP trunks between BCMs, between BCMs and legacy BCMs, or between BCM and Meridian 1-IPT and CS 1000/M	MMR transcoding JBIG transcoding

VoIP trunks for fallback configuration

This section gives an overview of VoIP trunks for fallback configuration.

Prerequisites for trunk fallback configuration

Perform the following tasks prior to the fallback configuration

- If you have not already done so, remember to define a route for the local PSTN for your own system so users can still dial local PSTN numbers.
- Ensure the PSTN and VoIP line pools have been configured before you continue with this section. For information about creating a VoIP line pool, see [VoIP trunk gateway configuration \(page 169\)](#). To configure PSTN lines, select Configuration > Telephony > Lines > Active Physical Lines.

VoIP interoperability—gatekeeper configuration

The following section describes the use of a gatekeeper for your H.323 VoIP trunks.

CS1000 as a gatekeeper

Both the BCM and the CS 1000 must be set to the parameters described in the following information for the gatekeeper to work effectively. Refer to *IP Peer Networking: Installation and Configuration* (553-3001-213) for detailed information on configuring a CS 1000 gateway.

For CS 1000, the Network Routing Service (NRS) can be configured and maintained through a web interface called NRS Manager. NRS Manager replaces the CS 1000 GK admin tool.

Review the following information before attempting to use the CS 1000 as a gatekeeper:

- Before a Gateway Endpoint registers with the CS 1000 gatekeeper it must first be added to the gatekeeper configuration.
- Before a registered Gateway Endpoint makes calls, it must have its routing entry information assigned within the gatekeeper configuration.
- Before any of these configuration changes become part of the gatekeeper active configuration, they must be committed to the active database.

BCM requirements CS1000 as GW

Set the BCM Local Gateway IP interface to the following using BCM Element Manager (go to Configuration > Resources > Telephony Resources > {Select IP Trunk} > H323 Settings tab):

- Set Call Signaling to GatekeeperRouted or GatekeeperResolved.
- Set Primary Gatekeeper IP to the IP address of the NRS.
- Set Alias Names to the Alias name that was used when the H.323 Endpoint for the BCM was created on the NRS.

To make a BCM 3.01 (or later)-to-CS 1000 call, ensure that the BCM routes and dialing plan (used to reach the CS 1000 systems) match the numbering plan entry assigned to the CS 1000 systems through NRS Manager.

Similarly, to make a CS 1000 system-to-BCM 3.01 (or later) call, ensure that the numbering plan entry assigned to the BCM (through NRS Manager) matches the dialing plan information configured on the CS 1000 systems.

CS 1000 configuration

You must use NRS Manager to configure the CS 1000.

The NRS server must be enabled and properly configured before any NRS data can be provisioned using NRS Manager. Refer to *IP Peer Networking: Installation and Configuration* (553-3001-213) for detailed information on configuring a CS 1000 gateway.

Private network—MCDN over PRI and VoIP specifications

This section gives specifications of MCDN networking over PRI and VoIP.

MCDN networking checklist

The following points provide a quick check for the system prerequisite settings for MCDN networking. Select the dialing plan to be used:

UDP (Universal Dialing Plan)

- DNs on the same node are dialed directly.
- DNs on other nodes are called by first dialing an Access Code and an ESN.
- Each node has its own ESN.

CDP (Coordinated Dialing Plan)

- DNs on all nodes are dialed directly.

Ensure the following common programming is configured:

- BCM Programming
- 1 Configure the system DN length to match the DN length used in the rest of the private network.
 - 2 Program the private Route: Type=Private, Dial=None.
 - 3 Enable the MCDN Supplementary Services; TRO=selected, ICCL=selected, TAT=selected.
 - 4 Program telephones with a target line that specifies the system DN of the telephone in the Private received number field.

Attention: If you have public DNs set up for your telephones that are different from the system-assigned DN, each telephone needs to use the public and private received digits on the target line.

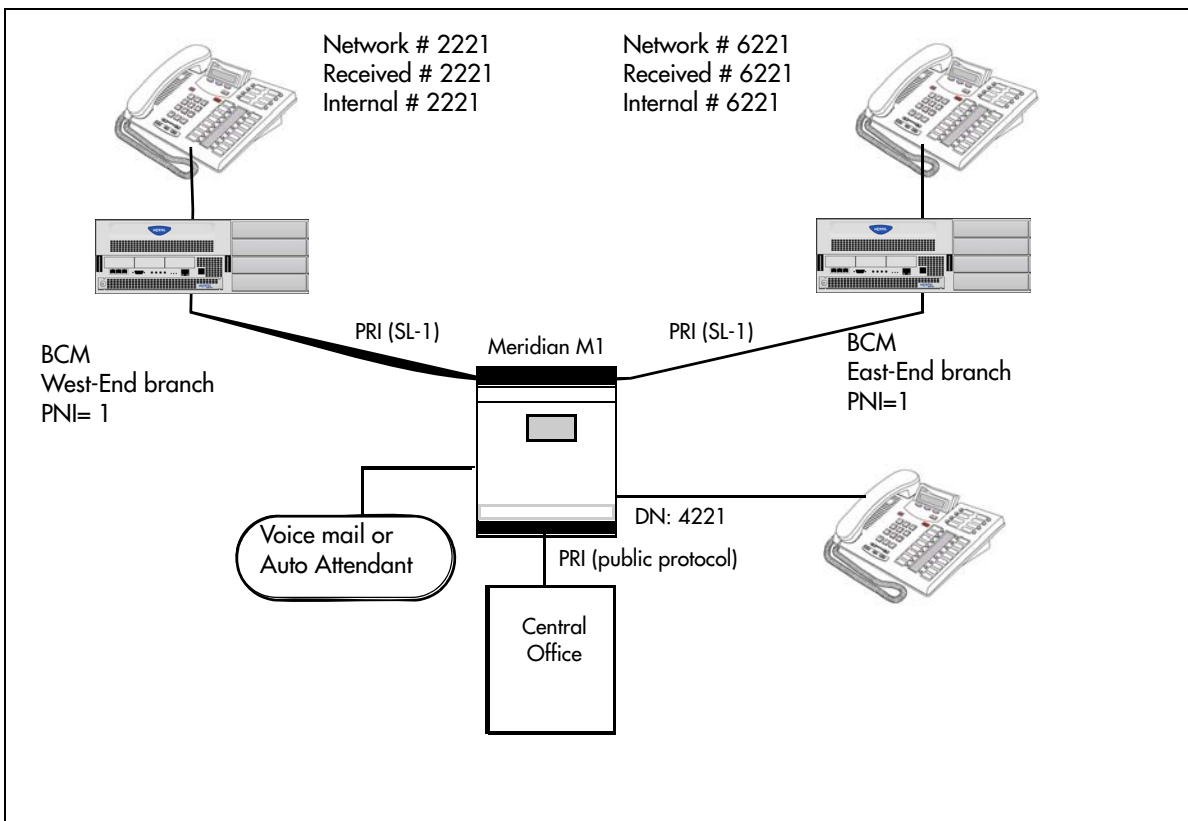
- Meridian 1 Programming
 - 1 Program the system PNI and the PNIs for the routes.
 - 2 Program the Meridian voice mailboxes (if required).
 - 3 Enable the MCDN Supplementary Services: RCAP=[ND2, TRO] or RCAP=[ND2,TRO,MWI], NASA=YES.

Set up the specific programming the system requires for the dialing plan. Refer to the following tables.

Example of private network with Meridian 1

The following figure shows a private network composed of one central Meridian 1, and two sites with BCM systems all connected by SL-1, with MCDN activated on all sites. This example uses a coordinated dialing plan (CDP). The DNs consist of four digits. The first digit is a destination code which is specific to each system. The last three digits are unique to each telephone within that system. Refer to [Dialing plan configuration for private networks \(page 83\)](#) for a description of the dialing plans available to private networks.

Figure 40 MCDN networking, with a common public network connection



Module programming for example

The following table lists the module settings that are required to set up the network.

Table 41 Module settings for MCDN network

West End office:		
Module programming	DTM	PRI
	Protocol	SL-1
	BchanSeq	Ascend
	ClockSrc	Primary External
East End office:		
Module programming	DTM	PRI
	Protocol	SL-1
	BchanSeq	Ascend
	ClockSrc	Primary External

MCDN dialing plan settings

The following table lists the dialing plan settings that are required to set up the network.

Table 42 MCDN dialing plan settings

West End office:		
Dialing Plan programming	Type	CDP
	Private Network ID	1
	Private received digit length	4
	Public received digit length	7
East End office:		
Dialing Plan programming	Type	CDP
	Private Network ID	1
	Private received digit length	4
	Public received digit length	7

Network routing information

The following table lists the lines and routing information required to set up the network shown in the figure in the previous section.

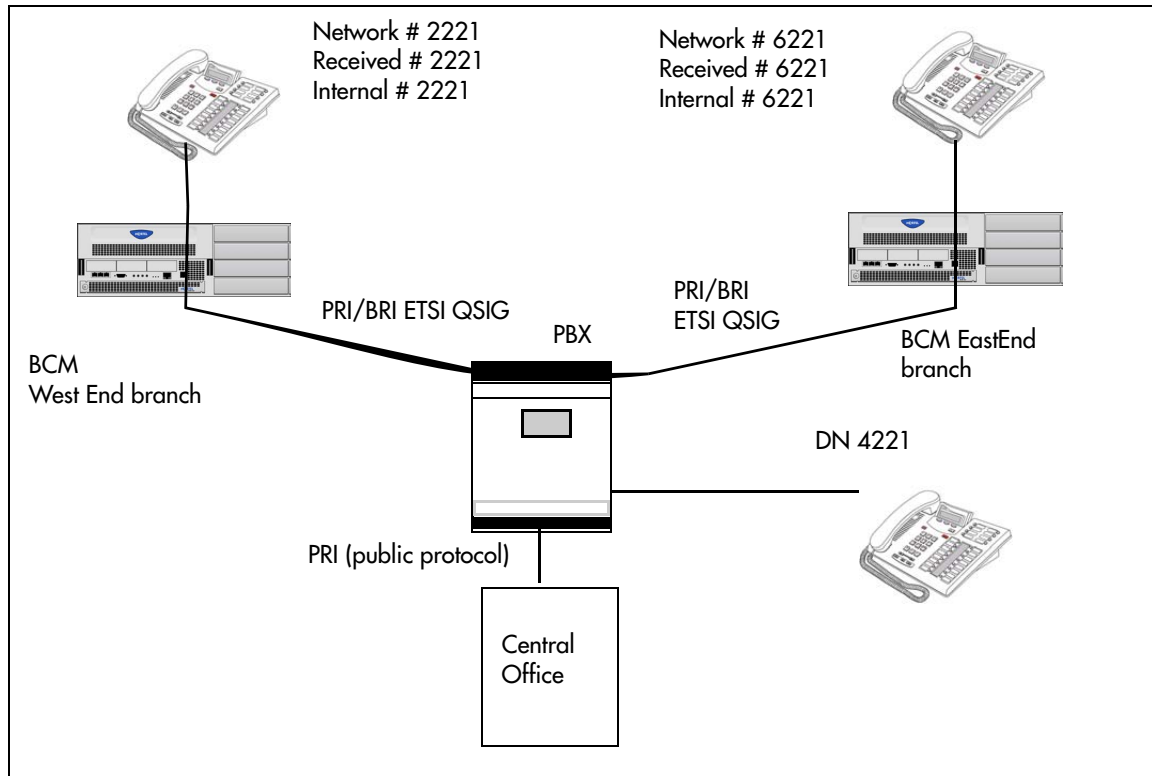
Table 43 Network routing information

West End office:			
Trunk/Line Data	Line 125	Target line	
	Private Received #	2221	
Line Access	DN 2221	L125:Ring only	
	Line pool access	Line pool BlocA	
Routing Services	Private Network		Public Network
	Head Office and East end		
Route	001		002
External #	No number		No number
Use	Pool BlocA		Pool BlocA
DN type	Private		Public
Destination codes for routes to:	Head office to M1	Head office to East End	
Destination Code	4 (includes steering code)	6	9
Normal route	001	001	002
Absorb	0	0	0
East End office:			
Trunk/Line Data	Line 125	Target line	
	Private Received #	6221	
Line Access	DN 6221	L125:Ring only	
	Line pool access	Line pool BlocA	
Routing Services	Private Network		Public Network
	Head Office to West End		
Route	001		002
Dial out #	No number		No number
Use	Pool BlocA		Pool BlocA
DN type	Private		Public
	Head Office to M1	Head Office to West End	Call terminates at M1
Destination Code	4 (contains location code)	2	9
Normal route	001	001	002
Absorb	0	0	0

Example of ETSI QSIG networking

The following figure illustrates an ETSI QSIG network.

Figure 41 ETSI QSIG networking



Hardware parameters for example

Settings for some of the hardware parameters for the ETSI QSIG networking example shown above are as follows:

West End office:				East End office:			
Hardware programming	DTM/BRIM	PRI/BRI		Hardware programming	DTM/BRIM	PRI/BRI	
	Protocol	ETSI QSIG			Protocol	ETSI QSIG	
	BchanSeq	Ascend (PRI only)			BchanSeq	Ascend (PRI only)	
	ClockSrc	Primary			ClockSrc	Primary	

T.38 fax

This section gives an overview of T.38 fax.

Prerequisites for T.38 fax configuration

If you are using the T.38 fax protocol, it is assumed that you have already configured IP trunks and gateways, and that they are functional. For more information on configuring VoIP trunks see [Line configuration overview \(page 15\)](#).

The T.38 fax protocol functions transparently with standard fax machines because it emulates a normal T.30 fax connection. Each endpoint of the IP trunk becomes a T.38 gateway. Both endpoints must support the T.38 fax protocol and have this feature enabled.

T.38 Fax operational parameters

Some fax machines cannot send faxes successfully over VoIP (T.38) trunks to the following destinations:

- CallPilot mailboxes
- CallPilot mailboxes accessed through auto-attendant
- Fax Transfer (calls transferred to a system fax device through the auto-attendant)

Use the following tips to avoid this problem:

- Avoid using manual dial on the originating fax machine. In some fax machines, dialing manually results in a much shorter call time-out.
- If you must dial manually, wait until the call is answered before you start the fax session.
- For Mailbox Call Answering only, if you must dial manually, enter the digit 8 as soon as you hear the mailbox greeting. This ensures that CallPilot initiates the fax session before the fax machine timer starts.

Attention: Enter the digit 8 for Norstar Voice Mail User Interface (NVMUI) only. To enable fax call answering when using CallPilot User Interface (CPUI), enter 707.

- Increase the call duration by adding a timed pause to the end of the dialing string. This addition allows the call to ring at the destination before the fax machine call-duration timer starts. Refer to your fax machine documentation for more information on how to insert pauses into dial strings.
- Because the problem is related to the delay in initiating the fax session, reduce the number of rings for fax mailboxes Call Forward No Answer (CFNA).

T.38 Fax restrictions

Voice mail and T.38 FoIP share Four fax ports, or up to eight fax ports if a CEC is installed in the BCM450 system.

If you allow fax messaging for the local VoIP gateway, you must be aware of the guidelines in [T.38 Fax operational parameters \(page 197\)](#) when you send and receive fax messages over VoIP trunks. For more information, see [VoIP trunk gateways \(page 173\)](#).

SIP fax over G.711

This section gives an overview of SIP fax over G.711. This feature allows fax to be transmitted using G.711 over SIP trunks in networks that contain SIP endpoint devices that do not support T.38 fax.

Prerequisites for SIP G.711 configuration

Perform the following prerequisites for SIP G.711 configuration:

- Configure IP trunks and gateways before you set up the G.711 fax protocol. For more information about configuring VoIP trunks, [Line configuration overview \(page 15\)](#)
- To configure this feature, designate the analog ports to which fax machines are connected as Modem rather than Telephone. This indicates to IP trunks that the bearer capability of these ports is 3.1 K audio.
- You can choose between T.38 or G.711 to transmit fax calls over SIP trunks. T.38 and G.711 are mutually exclusive. If you choose G.711 for fax transport, T.38 is not used. If you choose T.38, G.711 is not used.
- The choice between T.38 and G.711 is made on the SIP Media Parameters panel and applies to all SIP trunk calls.
- Both ends of the SIP call are responsible for “listening” for fax tones and configuring their G.711 tasks to transmit and receive fax reliably.

SIP G.711 operational parameters

Some fax machines cannot successfully send faxes over VoIP trunks to the following destinations:

- CallPilot mailboxes
- CallPilot mailboxes accessed through auto-attendant
- Fax Transfer (calls transferred to a system fax device through the auto-attendant)

Use the following tips to avoid this problem:

- Avoid using manual dial on the originating fax machine. In some fax machines, dialing manually results in a much shorter call time-out.

- If you must dial manually, wait until the call is answered before you start the fax session.
- For Mailbox Call Answering only, if you must dial manually, enter the digit 8 as soon as you hear the mailbox greeting. This ensures that CallPilot initiates the fax session before the fax machine timer starts.

Attention: Enter the digit 8 for Norstar Voice Mail User Interface (NVMUI) only. To enable fax call answering when using CallPilot User Interface (CPUI), enter 707.

- Increase the call duration by adding a timed pause to the end of the dialing string. This addition allows the call to ring at the destination before the fax machine call-duration timer starts. Refer to your fax machine documentation for more information on how to insert pauses into dial strings.
- Because the problem is related to the delay in initiating the fax session, reduce the number of rings for fax mailboxes Call Forward No Answer (CFNA).

SIP G.711 restrictions

If you allow fax messaging for the local VoIP gateway, you must be aware of the guidelines in [SIP G.711 operational parameters \(page 199\)](#) when you send and receive fax messages over VoIP trunks. For more information, see [VoIP trunk gateways \(page 173\)](#).

Attention: Fax tones that broadcast through a telephone speaker can disrupt calls on other telephones using VoIP trunks near the fax machine. Follow these suggestions to reduce the chance of your VoIP calls being dropped because of fax tone interference:
Position the fax machine away from other telephones.
Turn the speaker volume on the fax machine to the lowest level, or off.

Attention: Fax tones can be recorded in a voice mailbox. In the rare event that fax tones are captured in a voice mail message, opening that message from a telephone using a VoIP trunk can cause the connection to fail.

Meet Me Conferencing

This section gives an overview of Meet Me Conferencing. Meet Me Conferencing allows callers to establish a teleconference by calling in to a specified number at an agreed-upon time.

Prerequisites for Meet Me Conferencing configuration

Perform the following tasks to configure the system for Meet Me Conferencing:

- Informing conference users about Meet Me Conferencing. Refer to [How internal callers use Meet Me Conferencing \(page 201\)](#) and [How external callers use Meet Me Conferencing \(page 201\)](#)
- [System configuration for Meet Me Conferencing \(page 202\)](#)
- [Class of service configuration for Meet Me Conferencing \(page 205\)](#)

How internal callers use Meet Me Conferencing

Use Feature 985 to find the Meet Me Conferencing DN. Inform internal users that they can enter this DN directly or dial the Meet Me Conferencing feature code Feature 930.

Attention: After DN pool renumbering, the Meet Me Conferencing DN retains the same DN value, even though it is now outside the range of application DNs. You can renumber the Meet Me Conferencing DN to place it within the application DN range. See Renumbering DNs in the Device Configuration Guide (NN40020-300).

How external callers use Meet Me Conferencing

Configure other methods for external callers:

- Configure the Lines table for external access to the conference and advise chairpersons to include the external phone numbers in meeting invitations. For Lines table administration, see the *Call Pilot Manager Set Up and Operation Guide* (NN40090-300).
- Define a CCR tree transfer node that transfers callers to the Meet Me DN. For example, "Press 3 for Meet Me Conferencing". Advise chairpersons to include the transfer instructions in meeting invitations. For CCR tree

administration, see the *Call Pilot Manager Set Up and Operation Guide* (NN40090-300).

System configuration for Meet Me Conferencing

Follow Configuration > Applications > Meet Me Conferencing > Configuration to configure system and COS settings. See the following figure.

Figure 42 Meet Me Conferencing

COS ID	Name	Max Conference Size	Allow QuickStart	Allow Continue	Allow Announce Off	Conf Language
1		4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Primary
10		8	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Alternate
11		8	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Primary
12		8	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Alternate
13		10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Primary
14		10	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Alternate
15		10	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Primary
16		10	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Alternate
2		4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Alternate
3		4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Primary

The system settings apply to all conferences on the BCM.

Table 44 Meet Me Conferencing fields

Attribute	Value	Description
Welcome greeting - Company greeting ID	<Blank, or a Company Greeting number 1– 256> Default: Blank	The system plays the Welcome greeting for external callers. If the company greeting is blank, the system plays the standard greeting: “Welcome to the Meet Me Conferencing Service.” If you assign the company greeting, the administrator can select any existing Company Greeting to use as a Welcome greeting for this service. The administrator records and maintains these greetings using the voice mail administration interface.
Maximum chairperson wait time (min)	<1–120> Default: 20 minutes.	This attribute limits the amount of time that system resources can be tied up waiting for a conference to start. If the chairperson fails to log on within this limit, the system informs participants and terminates the conference. This limit is enforced on a for each participant. The timer starts after the last person joins the conference.
Maximum conference continuation time (min)	<1–999> Default: 120 minutes.	This attribute works with the Allow Continue option in the chairperson’s COS. If the Allow Continue option is enabled, the Maximum Conference Continuation Time limits the amount of time that system resources are used after the chairperson leaves the conference. When this limit expires, the system gives participants a 1-minute warning and then disconnects them. If the Allow Continue option is disabled, the conference ends when the chairperson leaves the conference.
Maximum conference limit time (hrs)	<1–24> Default: 12	This attribute limits the amount of time that system resources are used continuously for a single conference. This limit prevents a conference from going on indefinitely if multiple abandoned lines exist. The limit should be assigned to a reasonable time frame for BCM conferences. When this limit expires, the system gives participants a 1-minute warning and then disconnects them.

Table 44 Meet Me Conferencing fields

Attribute	Value	Description
Maximum last participant limit time (min)	<1–120> Default: 20 minutes	This attribute limits the amount of time that system resources are in use when the conference is reduced to a single participant. This limit prevents an abandoned line from tying up a port. Note: If you assign this setting to a value higher than the Maximum Conference Continuation Time, it has no effect because the system disconnects the conference when the Maximum Conference Continuation Time limit expires.
Authorization check period (days)	<0–365> Default: 60 days.	This attribute controls the Authorization Check feature. If assigned 0, the feature is disabled. Otherwise, the chairperson must change the PIN locally at least once during this period to maintain access. For a description of the PIN, see the <i>Meet Me Conferencing User Guide</i> (NN40020-104).
Class of Service Controls		
COS ID	<1–16>	The ID of the COS.
Name	<alphanumeric>	The name of the COS.
Max Conference Size	<4–18>	The largest number of participants (including the chairperson) that the chairperson can host, subject to resource availability.
Allow QuickStart	<check box>	The QuickStart option allows the conference to start without the chairperson. If you select this check box, the chairperson enables or disables the Quickstart feature in the chairperson administration menu. See the <i>Meet Me Conferencing User Guide</i> (NN40020-104). If you do not select this check box, the chairperson cannot enable the Quickstart option. The Quickstart option is disabled and does not appear in the chairperson administration interface.

Table 44 Meet Me Conferencing fields

Attribute	Value	Description
Allow Continue	<check box>	<p>If you select this check box, the chairperson can enable or disable the Conference Continuation option. The chairperson sets the Conference Continuation option during chairperson administration and during conference. See the <i>Meet Me Conferencing User Guide</i> (NN40020-104).</p> <p>If you do not select this check box, the chairperson cannot enable the Conference Continuation option. The option is disabled and does not appear in the chairperson administration interface or during the conference.</p>
Allow Announce Off	<check box>	<p>The Announcement settings are Tones, Names, and Off. The Off setting allows the chairperson to turn announcements off. See the <i>Meet Me Conferencing User Guide</i> (NN40020-104).</p> <p>If you select this check box, the value Off is offered as an Announcement setting within the chairperson administration menu and during conference.</p> <p>If you do not select this check box, the chairperson cannot change the Announcement option to Off. The Announcement option remains visible in the chairperson administration menu and during conference, but Off is not offered as a setting. The Announcement options are Tones and Names only.</p>
Conf Language	<drop-down list>	<p>The attribute specifies the language of the participant entry and exit, and warning voice prompts.</p> <p>If assigned <i>Primary</i>, the voice prompts play in the Primary language assigned in the VoiceMail system properties.</p> <p>If assigned <i>Alternative</i>, the voice prompts play in the Alternative language assigned in the VoiceMail system properties.</p>

Class of service configuration for Meet Me Conferencing

The administrator assigns each chairperson 1 of 16 Meet Me Conferencing COS values. The COS contains several settings that pertain to the operation of the feature. The default settings for each COS are listed in the following table. The Meet Me Conferencing COS is separate and distinct from the Mailbox COS. The administrator assigns a Meet Me Conferencing COS to a chairperson's DN.

Table 45 COS default settings

COS ID	Name	Max Conference Size	Allow QuickStart	Allow Continue	Allow Announce off	Conference Language
1	Name	4	X	—	—	Primary
2	Name	4	X	—	—	Alternate
3	Name	4	—	X	—	Primary
4	Name	4	—	—	X	Alternate
5	Name	6	—	—	—	Primary
6	Name	6	X	—	—	Alternate
7	Name	6	—	X	—	Primary
8	Name	6	—	—	X	Alternate
9	Name	8	—	—	—	Primary
10	Name	8	X	—	—	Alternate
11	Name	8	—	X	—	Primary
12	Name	8	—	—	X	Alternate
13	Name	10	—	—	—	Primary
14	Name	10	X	—	—	Alternate
15	Name	10	—	X	—	Primary
16	Name	10	—	—	X	Alternate

Ports overview

This section provides an overview of port ranges panel. The Port Ranges panel provides a list of which Ports are currently being used for RTP/UDP, UDP, and Signaling. In the case of RTP over UDP and UDP, it allows changes to the ports being used.

RTP over UDP and its uses

RTP over UDP is used by IP sets to connect to media gateways, and by IP trunks to connect to remote devices or PDM devices. All of these services require RTP over UDP. Each media gateway uses two ports. By default, RTP over UDP is set to use the port range 28000 - 28255. It is recommended that you keep 256 ports configured for RTP over UDP. The BCM requires a minimum of 110 ports to support necessary services. This includes up to 300 IP sets, 64 voice mail and contact center voice ports, and 130 trunks (with capacity expansion card [CEC] installed). Each of these devices requires two RTP over UDP ports.

You can configure up to ten separate ranges of ports.

UDP and its uses

UDP is used for T.38 Fax over UDP. By default, it uses the Range 20000 to 20255. You can configure up to ten separate ranges of ports. While the system can function with 12 ports, it is recommended that 256 ports are reserved.

Signaling ports and its uses

Signaling ports are used by the system and cannot be modified. They are provided to show where conflicts with UDP or RTP occur.

Media gateway overview

This section gives an overview of Media gateways.

Media gateways

Certain types of IP communications pass through Media Gateways on the BCM. You can control the performance of these communications by adjusting the parameters for echo-cancellation and UDP Redundancy.

For detailed information on configuring the Media Gateways, [Media Gateways panel \(page 211\)](#)

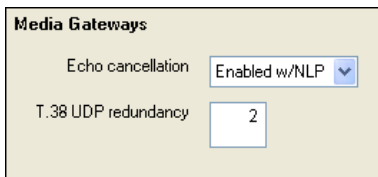
Media Gateways panel

This section gives an overview of Media Gateways panel.

Media Gateways panel

The Media Gateways panel allows you to set basic parameters that control IP telephony. The Media Gateways panel contains only two fields. To access the Media Gateways panel, click **Configuration > Resources > Media Gateways**.

Figure 43 Media Gateways panel



The screenshot shows a web interface titled "Media Gateways". It contains two settings: "Echo cancellation" with a dropdown menu set to "Enabled w/NLP", and "T.38 UDP redundancy" with a text input field containing the number "2".

Table 46 General Settings

Attribute	Value	Description
Echo Cancellation	<drop-down menu>	Enable or disable echo cancellation for your system.
	Enabled w/NLP	Default: Enabled w/NLP (check with your internet system administrator before changing this) Echo Cancellation selects what type of echo cancellation is used on calls that go through a Media Gateway. NLP refers to Non-Linear Processing.
	Enabled	
	Disabled	
T.38 UDP Redundancy	<numeric character string>	If T.38 fax is enabled on the system, this setting defines how many times the message is resent during a transmission, to avoid errors caused by lost T.38 messages.

Call security and remote access

This section provides an overview of Call security and remote access.

Call security and remote access

System restrictions are required to ensure that your system is used appropriately and not vulnerable to unauthorized use.

Call security includes

- restriction filters, which limit outbound call access
- remote access packages, which limit system call feature access for users calling in over the Private or Public network
- Class of Service codes, which require remote system users to enter a password before they can access the system. CoS passwords also can have restriction filters applied.
- [Remote access packages definitions \(page 219\)](#)
- [Direct inward system access \(page 217\)](#)
- [Remote access packages definitions \(page 219\)](#)

Refer to the following topics:

- [Restriction filters \(page 213\)](#)
- [Programming for remote call-in \(page 216\)](#)
- [Direct inward system access \(page 217\)](#)
- [Remote access packages definitions \(page 219\)](#)
- [CoS password definition \(page 220\)](#)

Call security works in conjunction with your dialing plan. Refer to [Dialing plan set-up \(page 35\)](#)

Restriction filters

Restriction filters allow you to restrict the numbers that can be dialed on any external line within BCM. Up to 100 restriction filters can be created for the system.

To restrict dialing within the system, you can apply restriction filters to:

- outgoing external lines (as line restrictions)
- telephones (as set restrictions)
- external lines on specific telephones (as line/set restrictions)

Restriction filters can also be specified in Restrictions service for times when the system is operating according to a schedule. Dialed digits must pass both the line restrictions and the set restrictions. The line per set (line/set) restriction overrides the line restriction and set restriction.

Programming for restriction filters

A restriction filter is a group of restrictions and overrides that specify the external numbers or feature codes that cannot be dialed from a telephone or on a line. The restriction filters setting allows you to assign restrictions in one step as a single package of dialing sequences that are not permitted.

In addition to restricting telephone numbers, you can prevent people from entering dialing sequences used by the central office (the public network) to deliver special services and features. Some of these features provide the caller with dial tone after they have entered the special code (which often uses # or *), therefore, users have an opportunity to bypass restrictions. To prevent this from happening, you can create filters that block these special codes.

You create a filter by defining the dialing sequences that are denied. There are also variations of each sequence that you want users to be able to dial, these are called overrides. Overrides are defined within each restriction package for each filter.

Once you create the filters, you can assign the restrictions to a telephone, to a line, to a particular line on a telephone, and to remote callers.

Attention: Filter 00 cannot be changed. Filter 01 has a set of defaults. Filters 02 to 99 can be set to suit your special requirements. See [Default filters for North America \(page 215\)](#).

- Each programmable filter can have up to 48 restrictions.
- There is no limit on the number of overrides that can be allocated to a restriction. However, there is a maximum total of 400 restrictions and overrides allocated to the 100 programmable filters.
- The maximum length of a restriction is 15 digits.
- The maximum length of an override is 16 digits.
- Entering the letter A in a dialing sequence indicates a wild card, and represents any digit from 0 to 9.

- You can use * and # in a sequence of numbers in either a restriction or an override. These characters are often used as part of feature codes for other systems or for features provided by the central office (the public network).
- When restricting the dialing of a central office feature code, do not forget to create separate restrictions for the codes used for DTMF and pulse lines (for example, *67 and 1167).
- Do not string together a central office feature code and a dialing sequence that you want to restrict. Create a separate restriction for each.
- You can copy restrictions and overrides from one filter to another. You can use a restriction or override in any number of filters. Each time you use a restriction or override, it counts as one entry. For example, if restriction 411 exists in filters 01, 02 and 03, it uses up three entries of the 400 entries available.
- Removing a restriction from a filter has no effect on the contents of other filters, even if the restriction was copied to them.
- You cannot delete a filter. Removing the restrictions programmed on a filter makes it an unrestricted filter but the filter itself is not removed.

Default filters for North America

Filter 00 permits unrestricted dialing and cannot be changed.

Filter 01 is pre-programmed with 10 restrictions and some associated overrides. In Filter 01, Restriction 02 and Override 001 allow long distance toll free calls.

The dialing string 911, which is the number for emergency assistance in North America, is included as both a restriction and an override in Filter 01. This arrangement prevents anyone from blocking calls for emergency assistance on lines or sets using the default filter.

Table 47 Default restriction filters

Filter	Restrictions (denied)	Overrides
00	Unrestricted dialing	
01	01: 0	
	02: 1	02: 1866
		001: 1800
		002: 1877
		003: 1888
	03: 911	001: 911
	04: 411	

Table 47 Default restriction filters

Filter	Restrictions (denied)	Overrides
01	05: 976	
	06: 1976	
	07: 1AAA976	
	08: 1900	
	09: 1AAA900	
	10: 5551212	
02 - 99	No restrictions or exceptions programmed	

Attention: Default filters are loaded when the system is initialized. A cold start restores the default filters.

Filters 02, 03, and 04, although not preset with restrictions and overrides, are the default filters in these programming headings:

Table 48 Default filters for program headings

Filter	Heading6	Sub-heading
02	System DNs	Set restrictions
03	Lines	Line restriction
04	Lines	Remote restriction

Default filters for all other jurisdiction.

Two profiles have global overrides which do not appear in Element Manager restriction programming and cannot be changed.

Australia: 000, 13144A

UK: 999, 112

Programming for remote call-in

There are three aspects to remote call ins:

- Setting up lines to allow users access to the system.
- Setting up Remote Access Packages that determine what services the remote users can access.
- Setting up CoS passwords for users calling in through the PSTN on lines programmed with DISA.

Direct inward system access

To control access from the public or private network, you can configure auto-answer trunks to answer with DISA. Remote callers hear a stuttered dial tone and must then enter a CoS password that determines what they are allowed to do in the system.

- Auto-answer T1 loop start and T1 E&M trunks are configured to answer with DISA by default.
- T1 DID trunks: You cannot configure T1 DID trunks to answer with DISA. If you want incoming T1 DID calls to be answered with DISA, configure the system with a DISA DN. Incoming T1 DID calls that map onto the DISA DN are then routed to a line that has DISA.
- You cannot program a DISA DN or Auto DN to VoIP trunks, because they act as auto-answer lines for private networks. However, you still need to assign remote access packages to the VoIP trunks, to ensure that remote access restrictions are properly applied to incoming calls trying to access the system or the system network.

Also refer to the following information:

- [Remote DISA line settings \(page 217\)](#)
- [Remote DISA on loop start trunks \(page 218\)](#)
- [Remote DISA on a T1 DID and PRI trunk \(page 218\)](#)
- [Remote DISA on DPNSS lines \(page 218\)](#)
- [Remote DISA on a private network \(page 219\)](#)

Remote DISA line settings

The remote access feature allows callers elsewhere on the private or the public network to access your BCM by dialing directly and not going through the attendant. After the remote user is in the system, they can use some of the system resources. You must enable remote access in programming before callers can use it.

BCM supports remote system access on a number of trunk types which may require the remote caller to enter a password for DISA.

The system resources, such as dialing capabilities, line pool access and feature access, that a remote user may access depends on the CoS password assigned to them. See [CoS password definition \(page 220\)](#).

Attention: Callers remotely access the BCM remote features setting by pressing * and the appropriate page code. See *Nortel Business Communications Manager 450 1.0 Configuration—Devices* (NN40160-500) for a list of feature codes.

Remote DISA on loop start trunks

Loop start trunks provide remote access to BCM from the public network. They must be configured to be auto-answer to provide remote system access.

A loop start trunk must have disconnect supervision if it is to operate in the auto-answer mode.

T1 E&M trunks always operate in disconnect supervised mode.

When a caller dials into the system on a line that has auto-answer without DISA, the system answers with system dial tone and no CoS password is required. In this case, the remote access package assigned to the line controls system capabilities.

When a caller dials in on a line that has auto-answer with DISA, the system answers with stuttered dial tone. This is the prompt to enter a CoS password that determines which system capabilities are available to the caller.

Remote DISA on a T1 DID and PRI trunk

Remote system access on T1 DID trunks is similar to that of T1 E&M trunks connected to a private network. The main differences are

- A remote caller is on the public network dialing standard local or long distance telephone numbers.
- Answer with DISA cannot be administered to a T1 DID and PRI trunk. You can program the dialed digits to match those of a specific target line DN, the DISA DN or the Auto DN. If you program the dialed digits to the DISA DN, only the incoming calls that match the programmed DN receive a DISA dial tone. Incoming calls with other digits are routed to a target line.

Remote DISA on DPNSS lines

A remote caller can access a BCM system dial tone, select a line pool that contains exchange lines or DPNSS lines, then dial a number. The procedure is identical to dialing an outside number from an extension in the local system. The main features are

- Calls coming from another switch to the BCM system are routed in two ways, depending on the Answer mode that you program. If the Answer mode is set to Manual, and the line is assigned to ring at an extension, the incoming call automatically rings at the assigned extension. If Answer mode is set to Auto, BCM automatically answers the incoming call. Because most other DPNSS features are extension-specific, Nortel recommends that all DPNSS lines are configured as auto-answer lines.
- The Page feature is available to both remote callers and callers within the system. A remote caller must have DTMF capability to access the Page feature.

- The line redirection feature allows the originating party to redirect a call that is waiting a connection or re-connection to an alternate destination after a time-out period. Failed calls can be redirected. Priority calls cannot be redirected.

Remote DISA on a private network

Systems connected to the private network deliver the last dialed digits to the destination BCM system for interpretation. The destination BCM system matches the digits to a target line or interprets the digits as a remote feature request. BCM then routes the call to the specified target line or activates the remote feature.

- By default, T1 E&M trunks are set to answer with DISA. For auto-answer T1 E&M trunks connected to a private network, change the default so that the trunks are not answered with DISA. If an auto-answer T1 E&M trunk is configured to answer with DISA, the system tries to interpret any received digits as a CoS password.
- The DISA DN and the Auto DN allow auto-answer private network and DID calls, in the same way that calls on auto-answer loop start and auto-answer T1 E&M trunks can be answered, with or without DISA. These DNs are described in [Dialing plan configuration for line pools and access codes \(page 91\)](#).
- Answer with DISA cannot be administered to a PRI trunk. Instead, you can program the dialed digits to match those of a specific target line DN, the DISA DN or the Auto DN on the other system.
- Answer with DISA cannot be administer to voice over IP (VoIP), since they do not connect systems outside the private network. However, a user calling in remotely on another system on the network can use the trunk to access the system or a user calling in on a PSTN line can use the trunk to access the private network. To provide control for this type of access, ensure that you specify remote access packages for the trunk.

Remote access packages definitions

The Remote access packages setting allows you to control the remote access to line pools and remote page.

Create a remote access package by defining the system line pools remote users can access. You then assign the package to individual lines, and to a particular Class of Service password. See [CoS password definition \(page 220\)](#).

CoS and DISA

The CoS password can define the set of line pools that may be accessed and whether or not the user has access to the paging feature.

The class of service (CoS) that applies to an incoming remote access call is determined by

- the filters that you apply to the incoming trunk
- the CoS password that the caller used to gain access to BCM.
- in cases where DISA is not automatically applied to incoming calls, the remote caller can change the class of service by dialing the DISA DN and entering a CoS password.

Remote users can access system lines, line pools, the Page feature, and remote administration. The exact facilities available to you through remote access vary depending on how your installer set up your system.

Attention: If the loop start line used for remote access is not supervised, auto-answer does not function and the caller hears ringing instead of a stuttered tone or the system dial tone.

CoS password definition

CoS passwords permit controlled access to the system resources by both internal and remote users.

- When an internal user enters a CoS password at a telephone, the restriction filters associated with the CoS password apply instead of the normal restriction filters.
- Similarly, when a remote user enters a CoS password on an incoming auto-answer line, the restriction filters and remote package associated with their CoS password apply instead of the normal restriction filters and remote package.

CoS password security and capacity

For security concerns, the following practices are recommended.

- Determine the CoS passwords for a system randomly and change them on a regular basis.
- Users should memorize their CoS passwords and keep them private. Typically, each user has a separate password. However, several users can share a password or one user can have several passwords.
- Delete individual CoS passwords or change group passwords when employees leave the company.
- A system can have a maximum of 100 six-digit CoS passwords (00 to 99).

To maintain the security of your system, the following practices are recommended:

- Warn a person to whom you give the remote access number to keep the number confidential.
- Change CoS passwords often.
- Warn a person to whom you give a CoS password, to memorize the password and not to write it down.
- Delete the CoS password of a person who leaves your company.

Attention: Remote users can make long distance calls. Remember that a remote user can make long distance calls that are charged to your company. They can also access line pools and make page announcements in your office.

External access tones

You can hear some of the following tones when accessing BCM from remote location. The following table shows the different types of tones and what they mean.

Table 49 External access tones

Tone	What it means
System dial tone	You can use the system without entering a CoS password.
Stuttered dial tone	Enter your CoS password.
Busy tone	You have dialed a busy line pool access code. You hear system dial tone again after five seconds.
Fast busy tone	<p>You have done one of the following:</p> <p>Entered an incorrect CoS password. Your call disconnects after five seconds.</p> <p>Taken too long while entering a CoS password. Your call disconnects after five seconds.</p> <p>Tried to use a line pool or feature not permitted by your Class of Service. You hear system dial tone again after five seconds.</p> <p>Dialed a number in the system which does not exist. Your call disconnects after five seconds.</p> <p>IP trunk lines do not produce tones when accessed from a remote location.</p>

DISA configuration for call security

This following describes the telephony configuration that allows users to call from a remote site into the system to access system features.

The following paths indicate where to access DISA settings in Element Manager and through Telset Administration:

- Element Manager:
 - Configuration > Resources > Telephony Resources
 - Configuration > Telephony > Dialing Plan > Public Network
 - Configuration > Telephony > Dialing Plan > Private Network
- Telset interface: **CONFIG > System prgrming > Access codes

Refer to the following:

- [Remote access control \(page 223\)](#)
- [Remote access control configuration \(page 224\)](#)

Remote access control

To control access from the public or private network, you can configure auto-answer trunks to answer with DISA. Remote callers hear a stuttered dial tone and must then enter a CoS password that determines what they are allowed to do in the system.

- Auto-answer T1 loop start and T1 E&M trunks are configured to answer with DISA by default.
- You cannot program a DISA DN or Auto DN to VoIP trunks, because they act as auto-answer lines for private networks. However, you still need to assign remote access packages to the VoIP trunks, to ensure that remote access restrictions are properly applied to incoming calls trying to access the system or the system network.

For specific line programming, refer to [Remote access control configuration \(page 224\)](#).

Remote access control configuration

Setting up remote access on different types of trunks requires you to understand the trunk properties and how you want the system to answer the dial-in calls.

Refer to the following information:

- [Configuration for loop start trunks \(page 224\)](#)
- [Configuration for a T1 DID trunk \(page 224\)](#)
- [Configuration for a PRI trunk \(page 225\)](#)
- [Configuration for DPNSS lines \(page 225\)](#)
- [Configuration for a private network \(page 226\)](#)

Configuration for loop start trunks

Loop-start trunks provide remote access to BCM from the public network. The trunks must be configured to be auto-answer to provide remote system access. Refer to [T1-loop start trunk configuration \(page 16\)](#)

A loop start trunk must have disconnect supervision if it is to operate in the auto-answer mode. T1 E&M trunks always operate in disconnect supervised mode.

When a caller dials into the system on a line that has auto-answer without DISA, the system answers with system dial tone and no CoS password is required. In this case, the restriction filters assigned to the line control system capabilities available to the caller.

When a caller dials in on a line that has auto-answer with DISA, the system answers with stuttered dial tone. This is the prompt to enter a CoS password that determines which system capabilities are available to the caller.

Configuration for a T1 DID trunk

Remote system access on T1 DID trunks is similar to that of T1 E&M trunks connected to a private network.

The main differences are

- A remote caller is on the public network dialing standard local or long distance telephone numbers.
- The digits received are delivered by the central office.

- DISA cannot be administered to a T1 DID trunk. You can program the dialed digits to match those of a specific target line DN, the DISA DN or the Auto DN. If you program the dialed digits to the DISA DN, only the incoming calls that match the programmed DN receive a DISA dial tone. Incoming calls with other digits are routed to a target line. Refer to [T1-E&M line configuration \(page 18\)](#), [T1-DID line configuration \(page 17\)](#).

Configuration for a PRI trunk

Remote system access on PRI trunks is similar to that of T1 E&M trunks connected to a private network.

The main differences are

- A remote caller is on the public network dialing standard local or long-distance telephone numbers.
- The digits received are delivered by the central office.
- Answer with DISA cannot be administered to a PRI trunk. Instead, you can program the dialed digits to match those of a specific target line DN, the DISA DN or the Auto DN.
- North America: Use incoming Call-by-Call (CbC) Service routing to map the call type to the DISA DN.
With FX, INWATS, 900, and SDS service types, either a Service Id (SID) or a CDN is mapped to Target Line Receive Digits. DISA may be accessed by having the SID or CDN map to the DISA DN. This example has a Receive Digit Length = 4, DISA DN = 1234, and CbC Routing with (Service Type = FX, Map from SID = 2, Map to digits = 1234). A call presented to the BCM system with service type FX and SID 2 are handled as follows:
 - The ISDN setup message specifies FX with SID = 2
 - The FX SID = 2 is mapped to DISA DN digits 1234
 - The call is answered with DISA.Refer to [PRI line configuration \(page 16\)](#).

Configuration for DPNSS lines

A remote caller can access a BCM system dial tone, select a line pool that contains exchange lines or DPNSS lines, and then dial a number. The procedure is identical to dialing an outside number from an extension in the local system. The main features are

- Calls coming from another switch to the BCM system are routed in two ways, depending on the Answer mode that you program. If the Answer mode is set to Manual, and the line is assigned to ring at an extension, the incoming call automatically rings at the assigned extension. If Answer mode is set to Auto, BCM automatically answers the incoming call. Because most other DPNSS features are extension-specific, Nortel recommends that you configure all DPNSS lines as auto-answer lines.

- The Page feature is available to both remote callers and callers within the system. A remote caller must have DTMF capability to access the Page feature.
- The line redirection feature allows the originating party to redirect a call that is waiting a connection or re-connection to an alternate destination after a time-out period. Failed calls can be redirected. Priority calls cannot be redirected.

Refer to [Private networking—DPNSS network services \(UK\)](#) (page 135).

Configuration for a private network

Systems connected to the private network deliver the last dialed digits to the destination BCM system for interpretation. The destination BCM system matches the digits to a target line or interprets the digits as a remote feature request. BCM then routes the call to the specified target line or activates the remote feature.

- By default, T1 E&M trunks are set to answer with DISA. For auto-answer T1 E&M trunks connected to a private network, change the default so that the trunks are not answered with DISA. If an auto-answer T1 E&M trunk is configured to answer with DISA, the system tries to interpret any received digits as a CoS password.
- The DISA DN and the Auto DN allow auto-answer private network and DID calls, in the same way that calls on auto-answer loop start and auto-answer T1 E&M trunks can be answered, with or without DISA.
- Answer with DISA cannot be administered to a PRI trunk. Instead, you can program the dialed digits to match those of a specific target line DN, the DISA DN or the Auto DN on the other system.
- Answer with DISA cannot be administer to voice over IP (VoIP), since they do not connect systems outside the private network. However, a user calling in remotely on another system on the network can use the trunk to access the system or a user calling in on a PSTN line can use the trunk to access the private network. To provide control for this type of access, ensure that you specify remote access packages for the trunk. This type of call is called a tandem call.

Additional configuration programming

This panel describes the telephony configuration that is used to control access to system lines by calls coming in from outside the system. The remote access package also allows remote paging capabilities.

Attention: Callers dialing into the system over private network lines are also considered remote callers.

The following paths indicate where to access remote access packages in Element Manager and through Telset Administration:

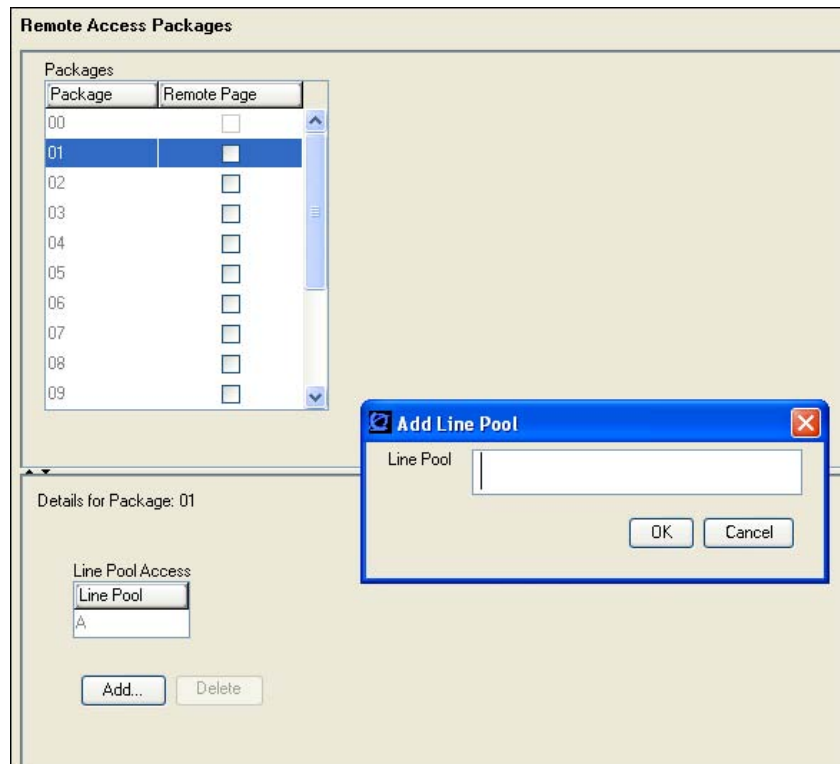
- Element Manager: **Configuration > Telephony > Call Security > Remote Access Packages**
- Telset interface: ****CONFIG > System prgrming > Remote Access**

Configuration for remote access packages

Use these panels to add allowed line pools to up to 99 remote access packages.

Remote access packages are assigned to lines and class of service (CoS) passwords. Lines used for private networking need remote access packages because calls coming from other nodes on the network are considered remote call-ins by your system.

Figure 44 Remote Access Packages tables



The following table describes each field on this panel.

Table 50 emote Access Packages

Attribute	Values	Description
Packages table		
Package	<00-99>	This designates the package number. This is what is entered in the fields for lines programming for remote access.
Remote Page	<check box>	Select check box if you wish to allow remote callers access to paging. Note: Remote paging is not supported on IP trunks.
Line Pool Access table		
Line pool	<A to O>/BlocA to F (PRI and VoIP)	Choose the line pool for which you want this package to be available.
Actions		
Add (line pool)	Package 00 is the default package and cannot be deleted. It provides no access to any line pools. On the Packages table, select the remote package number that you want to configure. Under the Line Pool Access table, click Add. In the Add dialog, enter a line pool. Click OK to save the pool. Next steps: Add remote access packages to lines and CoS passwords.	
Delete (line pool)	On the Packages table, select the remote package number where you want to delete line pools. On the Line Pool Access table select one or more line pools to delete. Click Delete. Click OK.	

The following is an example of how a remote access package works.

- Inbound PRI calls are on line pool BlocA
- Outbound calls are on analog lines using Pool A

If users coming in on the PRI are to be able to access outbound trunks on Pool A then the lines in BlocA must be in a remote package that allows access to Pool A.

Configuration for CoS passwords

The Class of Service panel allows you to configure passwords for system users who are dialing into the system over a PSTN/private network to use system features, or for users who must bypass local restrictions on telephones.

The following paths indicate where to access the Class of Service settings in Element Manager and through Telset Administration:

- Element Manager: **Configuration > Telephony > Call Security > Class of Service**
- Telset interface: ****CONFIG > Passwords > COS pswds**

CoS passwords permit controlled access to the system resources by both internal and remote users.

- When an internal user enters a CoS password at a telephone, the restriction filters associated with the CoS password apply instead of the normal restriction filters.
- Similarly, when a remote user enters a CoS password on an incoming auto-answer line, the restriction filters and remote package associated with their CoS password apply instead of the normal restriction filters and remote package.

Restriction filters for call security

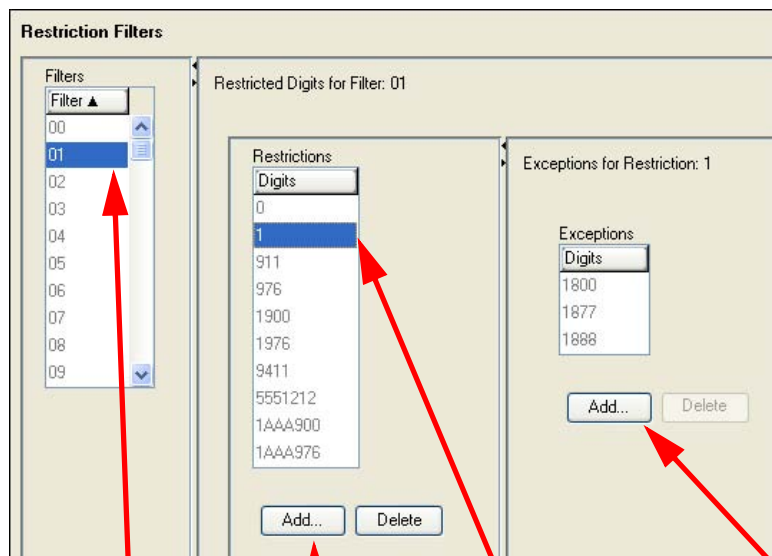
This section gives an overview of restriction filters for call security.

Restriction filters for call security

Restrictions are used to restrict outbound dialing. For example, restrictions can be applied to restrict dialing 1-900 numbers.

The restriction filters panel contains three list boxes. You progress from left to right as you populate the information. To access the Restriction Filters panel, click Configuration > Telephony > Call Security > Restriction Filters.

Figure 45 Restriction Filters panel



1. Select a restriction filter.

2. Add restricted digits to the Restriction filter.

3. If restricted digits have exceptions, select the digit.

4. Add exceptions.

Remote access packaging configuration

This section gives an overview of remote access packaging configuration.

Remote access packaging configuration

Refer to [Remote access packages definitions \(page 219\)](#)

LAN overview

On the BCM main unit, the LAN configuration determines how the Core Module of the BCM communicates with other devices on the LAN.

The following sections explain the concepts of the LAN on the BCM:

- [Definition and scope of a LAN \(page 235\)](#)
- [LAN configuration parameters \(page 235\)](#)
- [LAN DHCP configuration \(page 235\)](#)

Definition and scope of a LAN

The local area network (LAN) is a group of IP devices that can all communicate directly with each other over an IP network. Generally, all of these devices are in a small geographic range, such as a single office or building. The BCM allows you to connect several IP devices together on a LAN and then connect to the Internet or other LANs over a router.

LAN configuration parameters

LAN settings include determining IP and DNS settings and subnet settings. The LAN controls how the BCM behaves as a device on the IP network.

LAN DHCP configuration

By default, the BCM is assigned as a DHCP client. When the BCM starts, it sends a request for an address to a DHCP server. If no server responds, the BCM determines that no DHCP server is on the LAN and assigns the IP address to the last IP address received from the DHCP server (if the lease is valid) or to the default IP address (192.168.1.2).

Line configuration planning

The chapter [Line configuration overview \(page 15\)](#) provides an overview of line configuration concepts. The chapter [Line planning overview \(page 21\)](#) discusses planning for line configuration, including defining destination codes, and defining line pools. Complete the procedures in this chapter to assist in planning your line configuration.

Navigation

- [Defining line pools \(page 237\)](#)

Defining line pools

Line pools are groups of lines. Pooling lines allows you to use fewer lines than there are users. PRI lines and VoIP lines are always defined into line pools.

Prerequisites

- Line pools must never contain a mixture of lines. All lines in a given line pool should go to the same location
- Avoid putting unsupervised loop start lines in a line pool. These lines can become unusable, especially when a remote user uses the line pool to make an external call.
- Changes in the settings for trunk type on a system that is in use can result in dropped calls.

Procedure steps

Step	Action
1	To assign line pool access to telephones, select Configuration > Telephony > Dialing Plan > Line Pools .
2	To assign system-wide line pool access codes, select Configuration > Telephony > Dialing Plan > General (not applicable to Bloc pools).
3	Assign a line pool as the prime line. If the lines are idle, when the user lifts the receiver or presses Handsfree, use Automatic Outgoing Line selection to select any of the lines.
4	Consider your network configuration when assigning lines to line pools
5	Create a unified dialing plan by assigning lines to the same location to the same line pool on each of your systems. For example, if system A and system B each have TIE lines to system C, assign the TIE lines to pool D on each of the systems. Do not assign target lines to a line pool, as they are incoming-only.
<hr/> --End-- <hr/>	

BCM as a DHCP client

This section provides information on BCM as a DHCP client.

BCM as a DHCP client

The main module IP address can be statically assigned, or it can be a DHCP client. As a DHCP client, the Core Module receives an IP address from another DHCP server on the network. If no DHCP server is available, the Main Module uses the default IP address 192.168.1.2.

Data networking overview

The BCM is a converged voice product, and can be connected to virtually any data network, to provide Voice over Internet Protocol (VoIP) support in either a Local Area Network (LAN) or Wide Area Network (WAN) environment.

Data networking

On the BCM, data networking refers to both standard IP data networks, as well as VoIP. These two types of networks are closely intertwined, and connect a wide range of IP devices - including IP telephones and computers - with the BCM and with external networks.

BCM VoIP capability

The BCM provides VoIP functionality both within a LAN (Local Area Network), and across a WAN. It can contain IP telephones, which act similar to a traditional phone, but send their signals across data networks in the form of IP packets. The BCM can also contain IP trunks which connect offices together across an IP network.

For more information about VoIP see [VoIP overview \(page 163\)](#).

Configuration for BCM in data networking

To configure the BCM to work with a data network, complete the following steps:

- Complete the pre-installation checklist. This ensures that you've made all necessary preparations for connecting the BCM. For information on completing the pre-installation checklist, see [Data network prerequisites checklist \(page 245\)](#).
- Configure your router. If you already have a router on your system, you must make some modifications to its configuration for use with the BCM.
- Configure IP settings on the BCM. For information about configuring IP settings on the BCM, refer to [LAN overview \(page 235\)](#).
- Configure DHCP on the BCM. For information about configuring DHCP on the BCM, refer to [DHCP overview \(page 259\)](#).

BCM IP sub-system configuration

This section provides an overview of BCM IP sub-system configuration.

BCM IP sub-system configuration

The IP Settings define the basic and advanced IP address and DNS configuration for the BCM main unit.

The panel tabs links provide a general description of each panel and definitions of each panel field.

Data network prerequisites checklist

This section provides the specifications of Data network prerequisites checklist.

Navigation

- [Network diagram creation checklist \(page 245\)](#)
- [Network assessment checklist \(page 246\)](#)
- [Required keycodes checklist \(page 246\)](#)
- [System configuration for IP telephone functions checklist \(page 247\)](#)
- [VoIP trunks checklist \(page 247\)](#)
- [IP telephone records checklist \(page 248\)](#)

Network diagram creation checklist

To aid in installation, a network diagram provides a basic understanding of how the network is configured. Before you configure IP functionality, create a network diagram that captures all of the information described in the following table.

Table 51 Network diagram prerequisites

Prerequisites	Yes
Has a network diagram been developed?	
Does the network diagram contain any routers, switches or bridges with corresponding IP addresses and bandwidth values for WAN or LAN links?	
Does the network diagram contain IP Addresses, netmasks, and network locations for all BCM systems and other BCM products?	
Answer this if your system uses IP trunks; otherwise, leave it blank: Does the network diagram contain IP addresses and netmasks of any other VoIP gateways to which you must connect?	
Answer this only if your system uses a gatekeeper; otherwise, leave it blank: Does the network diagram contain the IP address for any Gatekeeper that may be used?	

Network assessment checklist

Answer the questions in the following table to ensure that the network is capable of handling IP telephony and that existing network services are not adversely affected

Table 52 Network assessment

Prerequisites	Yes	No
Has a network assessment been completed?		
Has the number of switch ports available and used in the LAN infrastructure been calculated?		
Does the switch use VLANs? If so, get the VLAN port number and ID.		
Have the used and available IP addresses for each LAN segment been calculated?		
Has DHCP usage and location been recorded?		
Has the speed and configuration of the LAN been calculated?		
Has the estimated latency values between network locations been calculated?		
Have the Bandwidth/CIR utilization values for all WAN links been calculated?		
Has the quality of service availability on the network been calculated?		

Required keycodes checklist

All elements of VoIP trunks and IP telephony are locked by the BCM keycode system. Answer the questions in Table 106 to ensure you have the appropriate keycodes.

Table 53 Keycodes

Prerequisites	Yes	No
Complete this question only if you are using VoIP trunks: Do you have enough VoIP keycodes? H.323 trunks use VoIP keycodes.		
Complete this question only if you are using IP telephones: Do you have enough IP client keycodes? (Note: IP clients and IP telephones are a 1:1 ratio. As soon as an IP telephone is registered, it occupies an IP client, whether it is active or not.).		
If you are using VoIP trunks, do you need to activate MCDN features? Note: If MCDN is already configured on your system for private networking over PRI lines, you do not need a separate MCDN keycode for VoIP trunks.		

System configuration for IP telephone functions checklist

Several sections of the BCM must be properly configured prior to IP telephony activation. Connect the BCM to the network before completing this checklist. Answer the questions in the following table to determine if your BCM has been correctly configured.

Table 54 BCM system configuration

Prerequisites	Yes	No
Is the LAN functioning correctly with the BCM? You can test this by pinging other addresses around the network from the BCM.		
Is the WAN functioning correctly with the BCM450?		
Have you determined the published IP address for the system?		
Have the necessary media gateway, IP client, and IP trunks resources been set?		
Has a dialing plan been created, taking into account special considerations for IP telephony and private and public networking?		
Have thresholds been set for desktop and soft client IP sets for voice quality monitoring with Proactive Voice Quality Management?		

VoIP trunks checklist

Answer the questions in the following table if you are configuring VoIP trunks.

Table 55 VoIP trunk provisioning

Prerequisites	Yes	No
Have you confirmed the remote gateway settings and access codes required?		
Have you determined the preferred codecs required for each type of trunk and destination?		
Have you set up line parameters, determined line pools for H.323 trunks, and set up destination codes? Have you determined which system telephones will have access to these routes?		
If you have not already assigned target lines, have you defined how you are going to distribute them on your system?		
Have you decided if you are going to employ the fallback feature? If yes, ensure that your routing and scheduling are set up. Ensure that QoS is activated. If either of these conditions is not met, your H.323 trunks will not work correctly.		

IP telephone records checklist

Answer the questions in the following table if you are installing i-series telephones.

Table 56 IP telephone provisioning

Prerequisites	Yes	No
Are IP connections and IP addresses available for all IP telephones?		
If DHCP is not being used, has all telephone configuration been documented and made available for telephone installers? Hint: Use the Programming Record form.		
If DHCP is not being used, or if you want to enter the port manually, has the VLAN port number been supplied, if one is being used on the switch?		
Have telephone power and connectors been provisioned?		
Do computers that will be using the Nortel Software Phone IP softphone 2050 meet the minimum system requirements, including headset? Note: Additional details available on client page for BCM		
Have DN records been programmed for the corresponding IP clients? (Use when manually assigning DNs to the telephones.)		

DHCP configuration

This section provides an overview of DHCP configuration.

The DHCP Server Settings contains fields to configure the BCM core as a DHCP server.

Use the following path to access DHCP server settings: **Configuration > Data Services > DHCP Server**.

The DHCP Server Settings panel is a multi-layered, multi-tabbed panel.

The panel tabs provide a general description of each panel and definitions of each panel field.

Click one of the following tabs:

- [DHCP server general settings tab](#)
- [IP Terminal DHCP Options tab](#)
- [Address ranges tab](#)
- [Lease information tab](#)

DHCP server general settings tab

The General Settings tab controls the main DHCP settings including WINS and DNS settings.

Figure 46 General Settings

DHCP Server

General Settings | IP Terminal DHCP Options | Address Ranges | Lease Info

DHCP server is: Enabled - IP Phones Only

IP domain name:

Primary DNS IP address:

Secondary DNS IP address:

WINS server address:

WINS node type: H-node

Default gateway: 192.168.2.4

Lease time (s): 604800

Figure 47 General Settings

DHCP Server

General Settings | IP Terminal DHCP Options | Address Ranges | Lease Info

Use DHCP Server on Integrated Router: ☐

DHCP server is: Disabled

IP domain name:

Primary DNS IP address:

Secondary DNS IP address:

WINS server address:

WINS node type: H-node

Default gateway: 192.167.131.1

Lease time (s): 604800

**WARNING Risk of loss of service**

When you change the default gateway, the DHCP server can become briefly unavailable to clients. When you make changes, consider doing so at a time that minimizes the effect on users.

Table 57 General Settings, DHCP server on main module

Attribute	Value	Description
DHCP Server is	Disabled Enabled - IP Phones Only Enabled - All Devices	DHCP server mode. If assigned <i>Enabled - All Devices</i> , the DHCP server provides service to all devices (IP phones and PCs). If assigned <i>Disabled</i> , the DHCP server on the CSC card is disabled.
IP domain name	<alphanumeric character string>	The domain name of the network.
Primary DNS IP address	<IP Address, format 10.10.10.10>	The IP address of the primary DNS to be used by DHCP clients.
Secondary DNS IP address	<IP Address, format 10.10.10.10>	The IP address of the secondary DNS to be used by DHCP clients.
WINS server address	<IP Address, format 10.10.10.10>	The address of the Windows Internet Server, which resolves IP addresses on a DHCP network.
WINS node type	<drop-down menu>	The type of WINS node: B-node: The BCM first checks the HMHOSTS cache, then uses broadcast for name registration and resolution. P-node: The BCM registers with a NetBIOS Name server at startup. M-node: Mixes B- and P-node. The BCM uses the B-node method, and if that fails, uses the P-node method. H-node: Uses both B- and P-node methods. B-node is used only as a last resort. Default: H-node
Default gateway	<IP Address, format 10.10.10.10>	The gateway through which DHCP clients connect to an external network. Generally, this is the IP address of the BCM router.
Lease time(s)	<numeric string>	The amount of time before a DHCP lease expires and the device must request a new IP address. Default: 604800 seconds

IP Terminal DHCP Options tab

The IP Terminal DHCP Options settings must be enabled for the IP Phones to function properly. If the system does not use IP Phones or if partial DHCP is enabled, this tab does not need to be configured.

The IP Terminal DHCP Options tab has three subpanels: Primary Terminal Proxy Server, (S1) Secondary Terminal Proxy Server (S2), and VLAN.

The Primary Terminal Proxy Server settings specify information that is sent with the DHCP lease, giving additional information to IP telephones.

The Secondary Terminal Proxy Server settings control a fallback option in the event that an IP phone is unable to connect with the Primary Terminal Proxy Server. The settings for the Secondary Terminal Proxy Server are the same as those for the Primary Terminal Proxy Server.

If you use a router that supports VLAN, you can configure the VLAN IDs that the IP phone should use. The system sends this identifier to all IP terminals along with the DHCP information.

Figure 48 IP Terminal DHCP Options

DHCP Server

General Settings | **IP Terminal DHCP Options** | Address Ranges | Lease Info

Primary Terminal Proxy Server (S1)

IP address: 192.167.131.40

Port: BCM

Port number: 7000

Action: 1

Retry count: 1

Secondary Terminal Proxy Server (S2)

IP address: 192.167.131.40

Port: BCM

Port number: 7000

Action: 1

Retry count: 1

VLAN

VLAN identifiers (comma-delimited):

Nortel WLAN Handset Settings

TFTP Server:

WLAN IP Telephony Manager 2245:

Table 58 IP Terminal DHCP Options

Attribute	Value	Description
Primary Terminal Proxy Server (S1)		
IP Address	<IP address> 10.10.10.10	The IP address of the Proxy Server for IP phones.
Port	<drop-down list>	Select the appropriate port: BCM SRG Meridian 1/Succession 1000 Centrex/SL-100 Other
Port number	<number>	The port number on the terminal through which IP phones connect.
Action	<read-only>	The initial action code for the IP telephone.
Retry count	<number>	The delay before an IP phone retries connecting to the proxy server.
Secondary Terminal Proxy Server (S2)		
IP address	<IP address> 10.10.10.10	The IP address of the Proxy Server for IP phones.
Port	<drop-down list>	Select the appropriate port: BCM SRG Meridian 1/Succession 1000 Centrex/SL-100 Other
Port Number	<number>	The number of the port IP sets use (read-only).
Action	<number>	(read only)
Retry Count	<number>	The amount of time, in seconds, before an IP set attempts to reconnect to the server.
VLAN		
Vlan identifiers (comma-delimited)	<number>	The VLAN values that are sent to all IP phones.
Nortel WLAN Handset Settings		
TFTP server	<IP address> 10.10.10.10	The address of the TFTP server that manages the WLAN handset firmware.
WLAN IP Telephony Manager 2245	<IP address> 10.10.10.10	The IP address of the WLAN IP Telephony Manager 2245.

Address ranges tab

The Address Ranges tab specifies IP addresses to be provided to DHCP clients. The Address Ranges tab has two tables: Included Address Ranges and Reserved Addresses. The Included Address Ranges specifies a range of IP addresses to be provided to DHCP clients.



WARNING Risk of loss of service

Whenever you make changes to the address range, the DHCP server may become unavailable to clients for a brief period of time. When making changes, consider doing so at a time that minimizes the effect on users. Whenever you make changes to the address range, the DHCP server may become unavailable to clients for a brief period of time. When making changes, consider doing so at a time that minimizes the effect on users.

Figure 49 Address Ranges tab

Table 59 Address Ranges

Attribute	Value	Description
Included Address Ranges		
From IP Address	<IP Address, format 10.10.10.10>	An IP address specifying the lowest IP address in a range.
To IP Address	<IP Address, format 10.10.10.10>	An IP address specifying the highest IP address in a range.
Add	<button>	Click to add an included address range.

Table 59 Address Ranges

Attribute	Value	Description
Delete	<button>	Click to delete a selected address range.
Modify	<button>	Click to modify a selected address range.
Reserved Addresses		
IP Address	<IP address>	Specify the IP Address that is reserved for this DHCP client.
MAC Address	<IP address>	Specify the MAC address for the DHCP client to which this IP address is assigned. The permitted values is 6 bytes in hexadecimal format.
Client Name	<alphanumeric>	Specify the name of the DHCP client.
Client Description	<alphanumeric>	Specify the description that helps to identify the DHCP client to which this IP address is assigned.
Add	<button>	Click to add a reserved address.
Delete	<button>	Click to delete a reserved address.

Lease information tab

The lease info panel is a read-only panel describing the current state of DHCP clients currently using the service. The Lease Info panel contains the Customer LAN Lease Info.

Figure 50 Lease Info

The screenshot shows the DHCP Server configuration window. The 'Lease Info' tab is selected, showing the 'Customer LAN Lease Info' section. Below this section, there are five read-only fields: IP Address, MAC Address, Client Name, Lease Start, and Lease Expiration.

Table 60 Lease Info

Attribute	Value	Description
IP Address	<read-only>	The IP address currently supplied to the client.
MAC Address	<read-only>	The MAC address of the client.
Client Name	<read-only>	The client name, if the client was given a name in the Reserved Addresses table. Otherwise, this field is blank.
Lease Start	<read-only date format: yyyy-mm-dd hh:mm:ss>	The date and time the lease began.
Lease Expiration	<read-only date format: yyyy-mm-dd hh:mm:ss>	The date and time the lease is set to expire.

VLAN overview

This section gives an overview of VLAN.

Overview to virtual LANs

A virtual LAN (VLAN) is a logical grouping of ports, controlled by a switch, and end-stations, such as IP telephones, configured so that all ports and end-stations in the VLAN appear to be on the same physical (or extended) LAN segment even though they may be geographically separated. VLAN IDs are determined by how the VLAN switch is configured. If you are not the network administrator, you must ask whoever manages the switch what the VLAN ID range is for your system.

VLANs aim to offer the following benefits:

- VLANs are supported over all IEEE 802 LAN MAC protocols, and over shared media LANs as well as point-to-point LANs.
- VLANs facilitate easy administration of logical groups of stations that can communicate as if they were on the same LAN. They also facilitate easier administration of move, add, and change in members of these groups.
- Traffic between VLANs is restricted. Bridges forward unicast, multicast, and broadcast traffic only on LAN segments that serve the VLAN to which the traffic belongs.
- For IP telephony, VLANs provide a useful technique to separate and prioritize the telephony traffic for L2 switches.
- VLAN also provides a shield from malicious traffic that may be targeted at the IP phone in order to steal or disrupt service.
- Reuse IP addresses in different VLANs.
- As far as possible, VLANs maintain compatibility with existing bridges and end stations.
- If all bridge ports are configured to transmit and receive untagged frames, bridges work in plug-and-play ISO/IEC 15802-3 mode. End stations are able to communicate throughout the Bridged LAN.

DHCP and VLAN

By using the BCM DHCP server, you can configure DHCP to auto-assign a VLAN ID to each IP telephone that registers. With this configuration, you can also choose to manually enter VLAN IDs, if you choose. The BCM DHCP server becomes the default VLAN that everyone can reach. The server provides the network configuration information in the default VLAN, and it also provides the VLAN information for the network.

Site-specific options for VLAN

The BCM DHCP server resides in the default VLAN and is configured to supply the VLAN information to the IP phones. The DHCP server supplies site-specific options in the DHCP offer message.

The following definition describes the Nortel IP Phone 2004-specific, site-specific option. This option uses the reserved for site specific use DHCP options (DHCP option values 128 to 254) and must be returned by the DHCP server as part of each DHCP OFFER and ACK message for the IP Phone 2004 to accept these messages as valid. The IP Phone 2004 pulls the relevant information out of this option and uses it to configure the IP phone.

Format of field is: Type, Length, Data.

Type (1 octet):

- Five choices 0x80, 0x90, 0x9d, 0xbf, 0xfb (128, 144, 157, 191, 251)
- Providing a choice of five types allows the IP Phone 2004 to work in environments where the initial choice may already be in use by a different vendor. Select only one TYPE byte.

Length (1 octet): (variable depends on the message content)

Data (length octets):

- ASCII based
- format: VLAN-A:XXX,YYY.ZZZ.
where VLAN-A: uniquely identifies this as the Nortel DHCP VLAN discovery.
-A signifies this version of this spec. Future enhancements could use -B, for example.
ASCII , (comma) is used to separate fields.
ASCII . (period) is used to signal end of structure.
XXX, YYY and ZZZ are ASCII-encoded decimal numbers with a range of 0-4095. The number is used to identify the VLAN Ids. A maximum of 10 VLAN Ids can be configured. NONE means no VLAN (default VLAN).

The DHCP Offer message carrying VLAN information has no VLAN tag when it is sent out from the DHCP server. However, a VLAN tag is added to the packet at the switch port. The packets are untagged at the port of the IP phone.

DHCP overview

On the BCM, DHCP can be set up in a variety of configurations, based on your needs, your existing network, and the version of the BCM that you have.

The following explains the various ways that you can configure DHCP on the BCM.

- [DHCP context in BCM450 \(page 259\)](#)
- [DHCP default configuration \(page 260\)](#)
- [DHCP server on the Main Module \(page 260\)](#)

DHCP context in BCM450

Dynamic Host Configuration Protocol (DHCP) is a protocol used to assign IP addresses to devices on an IP network dynamically. With DHCP, each device obtains a new IP address every time it connects to the network. DHCP allows a server to keep track of the IP addresses for all IP devices on the network.

On the BCM, DHCP reduces the complexity of configuring IP devices, particularly IP phones. Not only do IP phones receive an IP address through DHCP, they also receive additional information such as gateway and port information.

DHCP on BCM450

The BCM uses DHCP in a variety of ways. The core of the BCM has a DHCP server. In addition to providing IP addresses to devices on the LAN, this DHCP server also provides a DHCP address to the OAM port and to the DSP LAN.

In addition to these two DHCP components, the BCM also works with other DHCP devices that may already be on the network.

Main module DHCP client

The main module IP address can be statically assigned, or it can be a DHCP client. As a DHCP client, the Core Module receives an IP address from another DHCP server on the network. If no DHCP server is available, the Main Module uses the default IP address 192.168.1.2.

Main module DHCP server

The main module has a DHCP server that provides DHCP and vendor-specific information to IP sets. It also provides DHCP information to other devices on the LAN, in the event that no other DHCP Server, such as a router, is available.

DHCP default configuration

These network scenarios explain the BCM DHCP functionality.

BCM models

The default DHCP status is assigned to Enabled - IP Phones Only. By default, the BCM is a DHCP client. There are two cases.

DHCP server on the Main Module

On BCM450 models, the DHCP server is on the main module.

DHCP network scenarios

Refer to the following section:

- [BCM configured as DHCP client is unable to reach external DHCP server \(page 260\)](#)

BCM using a dynamic address is changed to a static address

If you manually change a dynamic IP address to a static IP address, the VoIP information for the BCM Lan changes as well.

For example, the S1 and S2 IP addresses for a BCM LAN are dynamically assigned to 47.166.50.80. If you change the BCM LAN IP address to the static IP address 47.166.50.114, the S1 and S2 IP addresses also change to 47.166.50.114. If you assign the S1 and S2 IP address manually, and the address is different from the BCM customer LAN address, these addresses are not updated.

BCM configured as DHCP client is unable to reach external DHCP server

If an external DHCP server is present in your network, the preferred configuration for the Main Module DHCP server is Enabled - IP phones only. In this case, the DHCP server provides configuration data to Nortel's IP phones only. All other devices, like PCs, receive the configuration data from the external DHCP server.

Changing the default router DHCP configuration

The DHCP Server supplies the Nortel specific information required by IP phones. This information includes TPS server information and VLAN IDs. If the S1 and S2 IP addresses retain their default values, the system automatically updates them when the router IP address changes. If the S1 and S2 addresses are entered manually, they are not automatically updated when the router IP address changes.

Dial Up overview

This section gives an overview of the key services of the dial-out interfaces on the BCM.

Remote access service

Remote Access Service (RAS) allows a client system to dial a telephone number and establish an IP link with a BCM. This link is a connection across a telephone network over an ISDN line, or between a modem on the client system and a modem on the BCM. Once this link is established, the client can run IP applications to access the BCM system's OAM server, Web Page Server or BCM Monitor.

A user must provide credentials to establish the PPP connection. The credentials used must match the ones of a BCM account which has the PPPLogin privilege.

Attention: The modem or ISDN interface must be enabled for a connection to take place.

The BCM can be configured with callback users along with their callback numbers. In this scenario, the user can ask BCM to callback before establishing the PPP connection. The BCM validates the user name and use the callback number associated with the account where the user name was found. The authentication is made using the user name and password associated with the account where the callback user name was found. The modem tries to call a configurable amount of time, with a configurable delay between attempts.

The BCM modem or ISDN interface automatically disconnect if there is no traffic on the IP link for a configurable amount of time.

The IP addresses assigned to the BCM and the remote client are configurable

- The default configuration for the modem dial-in is for the BCM to assign itself an address of 10.10.14.1 and assign to the remote client an address

of 10.10.14.2. The settings can be changed to have the remote client assign itself an address or even assign the BCM an address.

- The default configuration for ISDN dial-in is for the BCM to assign the first ISDN interface an address of 10.10.18.1 and the second client an address of 10.10.18.2. The first remote client is assigned 10.10.18.10 and the second client is assigned 10.10.18.11. The settings can be changed to have the remote clients assign themselves an address or even assign the BCM an address.

Finally, an administrator has the capability to disconnect a modem or ISDN call if they find that a modem or ISDN call is in progress.

To program the RAS configurable options, select:

- **Configuration > Resources> Dial Up Interfaces > Modem Dial-In Parameters**
- **Configuration > Resources> Dial Up Interfaces > ISDN Dial-In Parameters**

Modem remote access service specifics

For Modem dial in, the Auto-disable feature automatically disables the modem if no connections are established for a configurable period of time. The Auto-disable feature is turned off by default. The modem can be enabled through Element Manager, using Feature 9*8 or the Startup Profile. If the modem is enabled using the Startup Profile, the Auto-disable capability is turned off.

The modem has a Directory Number (DN) associated with it. This DN can be used to redirect a call to the modem. A call can be redirected to the modem DN using the F70 (Transfer) feature from any sets attached to the BCM, or it can be redirected to the modem DN using the Auto-Attendant feature. Any user on the BCM can redirect an active call at their set by using Feature 9*0 if they don't know the modem DN. Feature 9*0 also displays the modem DN on any sets with at least 1 line display.

The modem can also be programmed to answer incoming lines directly after a configurable number of rings. Please be aware that most modems are programmed by default to give up on a connection after 60 seconds. If the number of rings and the amount of time it takes for the 2 modems to establish a connection take more than 60 seconds, the connection fails. If an administrator wants a modem to answer after a longer period than this default timeout, the calling modem answer timeout should be changed accordingly.

Internal calls to the modem are always answered immediately. External calls transferred to the modem are answered after the number of rings specified on the Modem Dial-In Parameters tab. This gives enough time to wait and collect caller ID information, which is captured and logged every time the modem connects.

Automatic data dial-out service

Automatic Dial-Out Service allows IP communications with a remote server through the modem or ISDN interface.

The user can configure the BCM system to automatically set up a modem or ISDN connection with a remote PPP server for establishing a PPP link when it needs to deliver IP data packets. Many services on the BCM have destination or source addresses which could be resolved by a route associated with the Auto Dial-Out service. The SNMP Trap delivery service, Log download, Backup download, CDR records push, Software Updates pulls, and the Keycodes file upload are just examples of such services. An administrator must be aware that the use of scheduled services over the modem may not give the expected results as a modem connection could fail for many different reasons and besides the SNMP v3 trap delivery, those services have no retry capabilities.

The triggering IP data follows a configured IP route to access the PPP interface, which then activates a dialing script to cause the modem to dial a remote number, starts PPP negotiation, establishes PPP link, and delivers the data packets.

After a configurable period of inactivity over the PPP link, the modem or ISDN link is disconnected. Any new IP data packets then trigger the connection again. Please keep in mind the long distance charges when configuring the inactivity timeout. Sometimes it is cheaper to keep a link up a bit longer than to make two calls of shorter periods.

The number to dial has to be a number which can be dialed using a Destination Code (route). The modem or ISDN link cannot use a Line Pool access code to dial out.

The BCM uses the user name and password associated with the configured account to authenticate itself with the remote server.

The IP addresses assigned to the BCM and the remote server are configurable. Both must be resolvable with the routes programmed for dialing out and the remote server address must match the address supplied when programming the service that attempts to deliver the packets. More than one route can be programmed, but all use the same phone number to reach the remote server.

To program the Automatic Data Dial-Out configurable options in Element Manager, select Configuration > Resources > Dial Up Interfaces > Dial-Out Interfaces.

Modem compatibility

The internal modem is compatible with all V.34 modems, and has been tested with the following modems:

- U.S. Robotics Sportster 33.6 FaxModem (external modem)
- Microcom DeskPorte 28.8P (external modem)
- PCTEL 2304WT V.92 MDC (internal modem Dell Portable)
- U.S. Robotics Sportster 56K (external modem)

ISDN planning and engineering

This section gives an overview of ISDN planning and engineering.

ISDN standards compatibility

In North America, BCM ISDN equipment supports National ISDN standards for basic call and calling-line identification services. BCM BRI is compliant with National ISDN-1 and PRI is compliant with National ISDN-2.

BCM does not support EKTS (Electronic Key Telephone System) on PRI.

In Europe, BCM supports ETSI Euro and ETSI QSIG standards, and PRI SL-1 protocol.

ISDN network planning

For ISDN BRI service, your service provider supplies service profile identifiers (SPIDs), network directory numbers (Network DNs), terminal endpoint identifiers (TEIs), and other information as required to program your BCM, TE and other ISDN equipment.

BCM does not support any package with EKTS or CACH. EKTS is a package of features provided by the service provider and may include features such as Call Forwarding, Link, Three-Way Calling, and Calling Party Identification.

Ordering ISDN PRI

The following describes how to order ISDN PRI service for your BCM.

Ordering ISDN PRI service in Canada.

Ordering ISDN PRI service in Canada/United States from your service provider. Set the BCM equipment to the PRI protocol indicated by your service provider

Outside Canada and the United States, order Euro ISDN PRI and/or BRI service from your service provider. Set the BCM equipment to the Euro ISDN protocol.

Ordering ISDN BRI

The following provides information about how to order ISDN BRI service for your BCM.

In Canada, order Microlink service, the trade name for standard BRI service. You can order either regular Microlink™ service, which includes the CLID feature, or Centrex Microlink™, which includes access to additional ISDN network features, including Call Forwarding.

When ordering Microlink™ service, it must be ordered with EKTS turned off. If you will be using a point-of-sale terminal adapter (POSTA), ask for D-channel packet service to be enabled.

In the United States, regardless of the CO (Central Office) type, order National ISDN BRI-NI-1 with EKTS (Electronic Key Telephone System) turned off. Use the following packages as a guideline for ordering your National ISDN BRI-NI-1. However, Nortel recommends using packages M or P with the BCM system. Contact your service provider for more information about the capability packages it offers. Bellcore/National ISDN Users Forum (NIUF ISDN packages supported by BCM (for ordering in U.S.).

	Capability	Feature set	Optional features	Point-of-sale	Voice	Data
M	Alternate voice/circuit-switched data on both B-channels		CLID		x	x
P	Alternate voice/circuit-switched data on both B-channels D-channel packet	flexible calling for voice (not supported by BCM) Basic D-Channel Packe	additional call offering (not supported by BCM) calling line identificati on	x	x	x

If you want to transmit both voice and data and support D-channel packet service, order package P. However, BCM does not support the flexible calling for voice and additional call-offering features that are included in package P.

Multi-Line Hunt may be ordered with your package. When a telephone number (the Network DN) in the group of numbers assigned by your service providers is busy, the Multi-Line Hunt feature connects the call to another telephone

number in the group. BCM supports the feature only on point-to-point, network connections (T loop). Check with your service provider for more information about Multi-Line Hunt.

Any of the ISDN packages allow you to use sub-addressing, but your ISDN TE must be equipped to use sub-addressing for the feature to work.

Outside Canada or the United States, order Euro ISDN PRI or BRI service, or both, from your service provider. Set the BCM equipment to the Euro ISDN protocol.

Supported ISDN protocols

The switch used by your service provider must be running the appropriate protocol software and the correct version of that software to support ISDN PRI and BRI. Each protocol is different and supports different services. Contact your service provider to make sure that your ISDN connection has the protocol you require.

Setting up a dialing plan

Dialing plans allow users to access the public network, to make calls, and to answer dial strings.

Planning the use of destination codes

Because the system checks the initial digits of a call against the routing tables, each type of internal or external call must begin with a unique pattern of digits.

To build a route to allow local calls, use the following procedure.

Procedure steps

Step	Action
1	Click Configuration > Telephony > Dialing Plan > Routing .
2	Create a route that uses the line pool you assigned for the PSTN trunks
3	Create a destination code record and enter a destination code, such as 9, which is a common local call code. Refer to Grouping destination codes using a wild card (page 59) The destination code can use a different route, depending on what schedule is assigned. In the current example, the route you define is used when someone dials 9 during Normal mode, when the other Schedules are turned off.
4	Set up the Normal schedule with the route number you defined in step 1.
--End--	

Procedure job aidInitial digits assignment

The following table gives a sample plan for how initial digits are assigned in a network of systems with three-digit intercom numbers.

Table 61 Leading digit assignments

Leading Digits	Use
0	Network Direct Dial
221-253	Intercom calls
4	Coordinated Dialing Plan
5	Unused
6	Unused
1	Call Park Prefix
9	All PSTN Calls
7	Unused

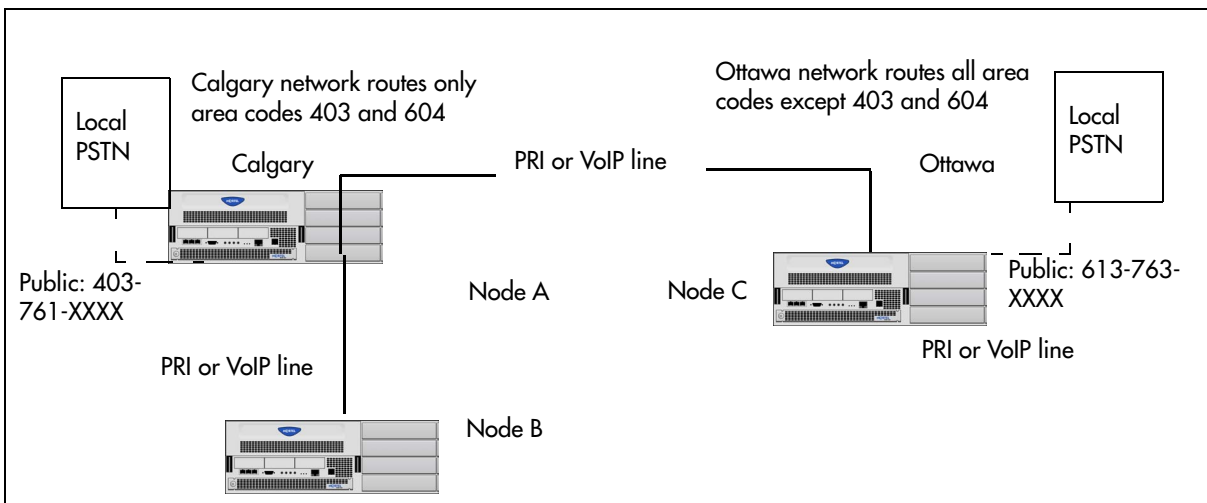
Private network—PRI and VoIP tandem network specifications

This section provides specifications for PRI and VoIP tandem network.

Example private tandem network of BCMs

The following figure demonstrates a tandem configuration.

Figure 51 Private tandem network of BCMs



Destination codes, external terminating calls

The following tables show the routing tables for Node A and Node C for external and internal terminating calls.

Table 62 Node A destination code table, external termination

Route	Absorb length	Destination code (public DNs)
4 (PSTN)	1	91604
3 (Node B)	0	91403762 (Node B)
4 (PSTN)	1	9140376* (not internal network)
* This wild card represents a single digit.		

Table 62 Node A destination code table, external termination

Route	Absorb length	Destination code (public DNs)
4 (PSTN)	1	<u>9</u> 14037* (not internal network)
4 (PSTN)	1	<u>9</u> 1403* (not internal network)
4 (PSTN)	1	<u>9</u> * (not internal network)
* This wild card represents a single digit.		

Table 63 Node C destination code table, external termination

Route	Absorb length	Destination code (Public DNs)
3 (Node B)	0	<u>9</u> 1613764 (Node D)
3 (Node B)	0	<u>9</u> 1613766 (Node F)
4 (PSTN)	1	<u>9</u> 161376* (not internal network)
4 (PSTN)	1	<u>9</u> 16137* (not internal network)
4 (PSTN)	1	<u>9</u> 1613* (not internal network)
4 (PSTN)	1	<u>9</u> 161* (not internal network)
4 (PSTN)	1	<u>9</u> 16* (not internal network)
4 (PSTN)	1	<u>9</u> 1* (not internal network)
4 (PSTN)	1	<u>9</u> (not internal network)

Dialing plan and routing specifications

The following chapter provides reference to the configuration of the lines and loops to allow system users to dial out of the system over a public or private network.

Destination code leading digits

the following table gives a sample plan for how initial digits are assigned in a network of systems with three-digit intercom numbers.

Table 64 Destination code leading digits

Leading Digits	Use
0	Network Direct Dial
221-253	Intercom calls
4	Coordinated Dialing Plan
5	Unused
6	Unused
1	Call Park Prefix
9	All PSTN Calls
7	Unused

Meridian 1 access versus BCM access codes

Three special access codes exist specifically for programming calls over PRI and VoIP trunks that are using the MCDN protocol, and which connect to a call servers that use specific call codes for special call types, such as the Meridian 1 (M1). The purpose of the codes is to allow easier programming of the call servers when calls are tandemed through a BCM system to the local PSTN. Refer to “Private Network Settings” on page 290 for a description of these fields in context with the private dialing plan.

The following table shows how the codes relate.

Table 65 Meridian 1 and BCM access codes comparison matrix

Meridian 1 access codes	BCM access codecs	sample code
Network/long distance code	Private access code	6
	National access code	61
Local code	Local access code	9
	Special access code	9

Routing service record, public line pool

The following figure provide examples of how you can record dialing plan information in a spreadsheet. The example shows dialing plan information for a Toronto system in a network of three offices: Toronto, Halifax, and Vancouver. Without routing, a BCM user in Toronto must to select a line pool and dial 1-902-585-3027 to reach extension 27 in Halifax (902). By creating a destination code of 30 and creating a route that uses the proper line pool and dial out number, the user simply dials 3027. The same feature is available for Vancouver (604).

Figure 52 Routing service record: use pool

Routing Services (Services: Routing Service)		
Route # (000-999)	Dial-out (if required) (max. 24 digits or characters)	Use Pool
100	902-585	ABC
101	902-585	ABC
102	604-645	ABC
103	604-645	ABC

Create unique
route number

Specify dial-out digits

Route through Pool A

Routing service record, destination code

The following figure provide examples of how you can record dialing plan information in a spreadsheet. The example shows dialing plan information for a Toronto system in a network of three offices: Toronto, Halifax, and Vancouver. Without routing, a BCM user in Toronto must to select a line pool and dial 1-902-585-3027 to reach extension 27 in Halifax (902). By creating a destination code of 30 and creating a route that uses the proper line pool and dial out number, the user simply dials 3027. The same feature is available for Vancouver (604)

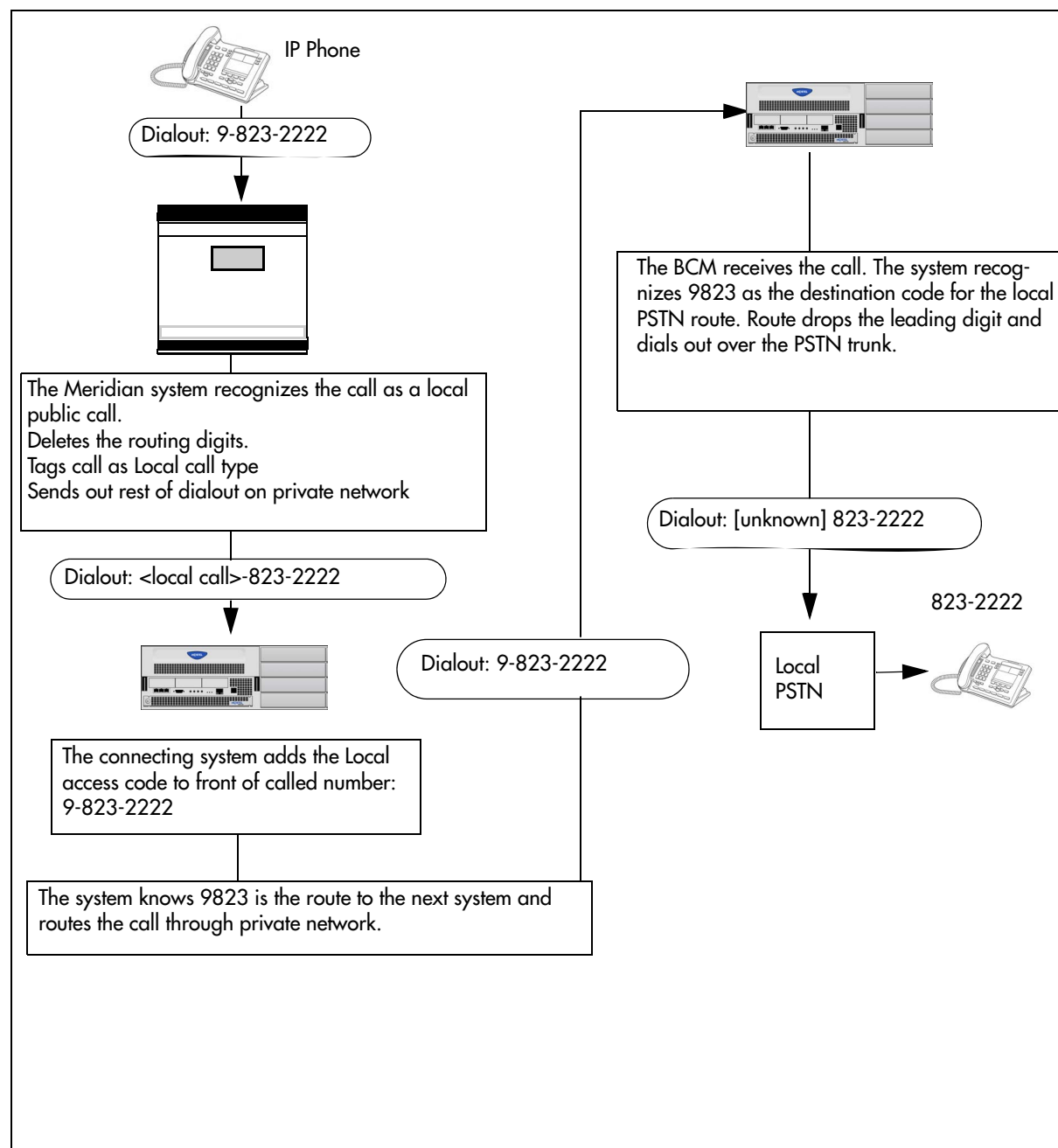
Figure 53 Routing service record: Destination code

Routing service (continued)								
Dest code (Services: Routing Services: Dest Codes)								
Service Schedule	Normal		Schedule					
DestCode (max. 12 digits)	Use route (001-999)	Absorb Length	1st route (001-999)	Absorb Length	2nd route (001-999)	Absorb Length	3rd route (001-999)	Absorb Length
30	100	0	000	All	000	All	000	All
31	101	0	000	All	000	All	000	All
32	102	0	000	All	000	All	000	All
33	103	0	000	All	000	All	000	All

Create unique code Specify which route to use Add Destination code to dialout out string

Tandem call progression

The following figure charts the process for a call tandeming through a BCM to the local public network.

Figure 54 Local call tandemed through private network nodes

Dialing plan—routing and destination codes specifications

This section provides the specifications of destination code schedules and second dial tone values for setting up the dialing plan.

Destination codes schedules

The following table describes the fields on the Destination codes frame. To access destination code schedules, click **Configuration > Telephony > Dialing Plan > Routing > Destination Codes**.

Table 66 Destination codes schedules

Attribute	Value	Description
Schedule	Defaults: Night, Evening, Lunch, Weekend, Sched. 5, Sched. 6	If you use a different carrier at different times of the day or week, you can set the destination code to use that route and provide two more backup routes. The user does not experience any difference in dialing sequence.
First Route	<configured route #>	This is the route that the system uses, during the indicated schedule, when the destination code is added to the dial string.
Absorbed Length	All, None, 1-X	This indicates how much of the destination code gets removed before the system sends the dial string to the network.
Second Route	<configured route #>	This is the route the system uses if the first route is unavailable.
Absorbed Length	All, None, 1-X	This indicates how much of the destination code gets removed before the system sends the dial string to the network.
Third Route	<configured route #>	This is the route the system uses if the first and second route are unavailable.
Absorbed Length	All, None, 1-X	This indicates how much of the destination code gets removed before the system sends the dial string to the network.

Second dial tone values and descriptions

The following table provides the Second dial tone values.

Table 67 Second dial tone

Attribute	Value	Description
SDT Prefix List		
SDT Prefixes		Enter the digits to match to trigger a second dial tone.
Actions		
Add	Button	Select to add an SDT prefix.
Delete	Button	Select an SDT prefix from the list and click delete to remove from the list.

Private network—DPNSS network services (UK) specifications

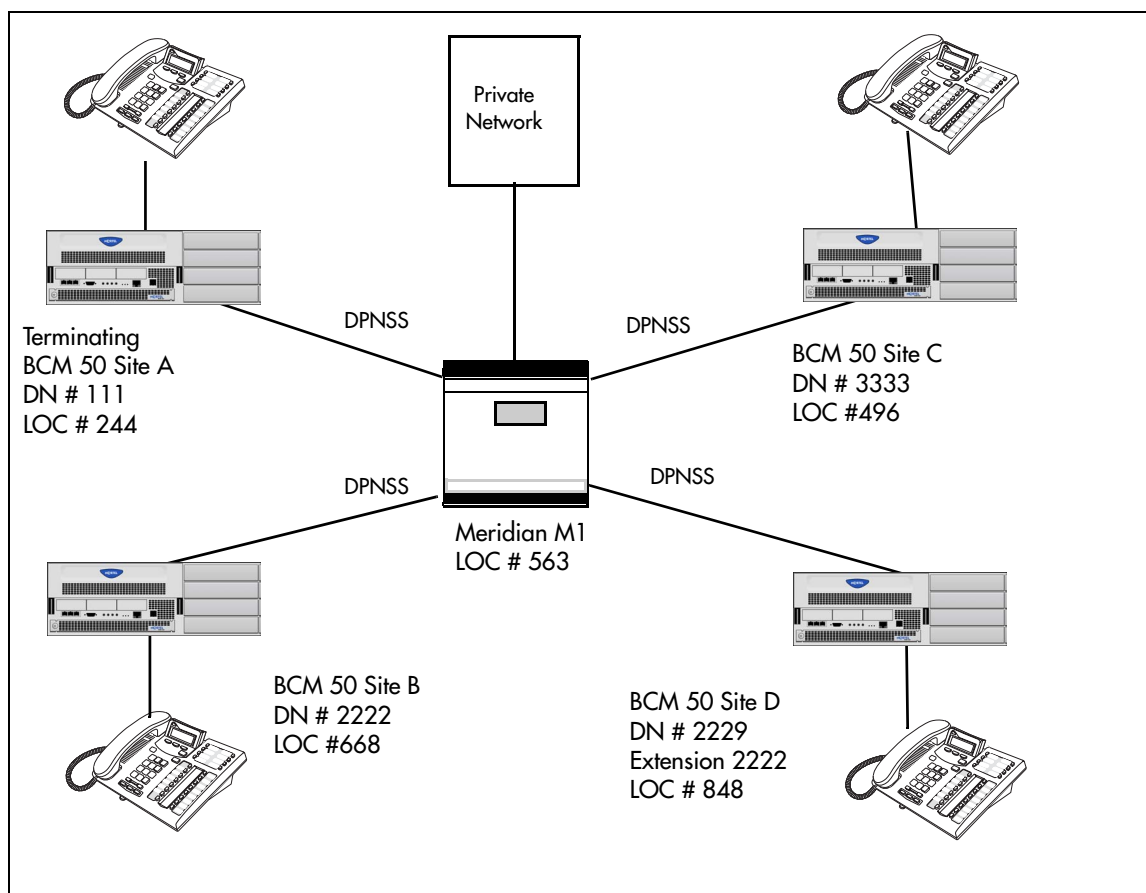
This section gives the specifications for DPNSS services.

Example of Private network with DPNSS

A typical Private Number, using a private access code and dialed from another site on the network, appears in the following table.

Private Access Code	+ Home Location Code	+ Directory Number	= Calling Party Number
6	+ 848	+ 2222	= 6-848-2222

In this networking example, a private network is formed when several systems are connected through a Meridian M1 and a terminating BCM system. Each site has its own HLC and a range of DNs. The following figure illustrates this example.

Figure 55 DPNSS networking

Calling number values for network example

The following table shows examples of the construction of numbers used when dialing within the example network. Note that 6 is the Private Access code.

Table 68 Calling numbers required for DPNSS network example

Calling site	LOC/HLC	Calling party number	Called site	Dialing string	Called party number
Site A	224	244 1111	Site B	6 688 2222	688 2222
Site B	688	688 2222	Site D	2 848 2222	848 2222
Site D	848	2222	Site D	22229	2229
Site C	496	496 3333	Public DN	9 563 3245	563 3245

Routing description for network example

The following table shows examples of the routing required to set up the network shown in the preceding figure. Note that 6 is the Private Access code

Table 69 Routing for DPNSS network

Private Network: (for each branch BCM)			
Routing service to		Private network	Public network
	Route	001	002
	Dial out #	No number	No number
	Use	Pool N	Pool N
	DN type	none (private access code 6 is programmed)	public
	Destination Code	6	9
	Normal route	001	002
	Absorb	1	1

Guidelines for private DPNSS network dialing plan

Use the following guidelines when creating a private dialing plan with DPNSS:

- When creating HLCs for the nodes in your system, avoid numbering conflicts between network nodes and internal DNs, Hunt group DNs.
- Program a Private Access Code into your destination routing tables to avoid conflicts with your internal HLC and dest code dialing plan. For example, if a dialout HLC is 848, but this number already exists in the BCM system for an extension, the routing tables should add a Private Access Code to the dest code. If the code is programmed as 6, the dest code becomes 6848. 6848 uses a route to dial out 848 using the DPNSS line pool, allowing the call to be placed.

Attention: Private Access Code is required only for specific DPNSS features such as Diversion, Route Optimization, and Redirection.

VoIP trunk gateway specifications

Refer the following section for VoIP trunk gateway specifications.

T.38 fax protocol restrictions and requirements

The following table is a list of restrictions and requirements for the T.38 fax protocol.

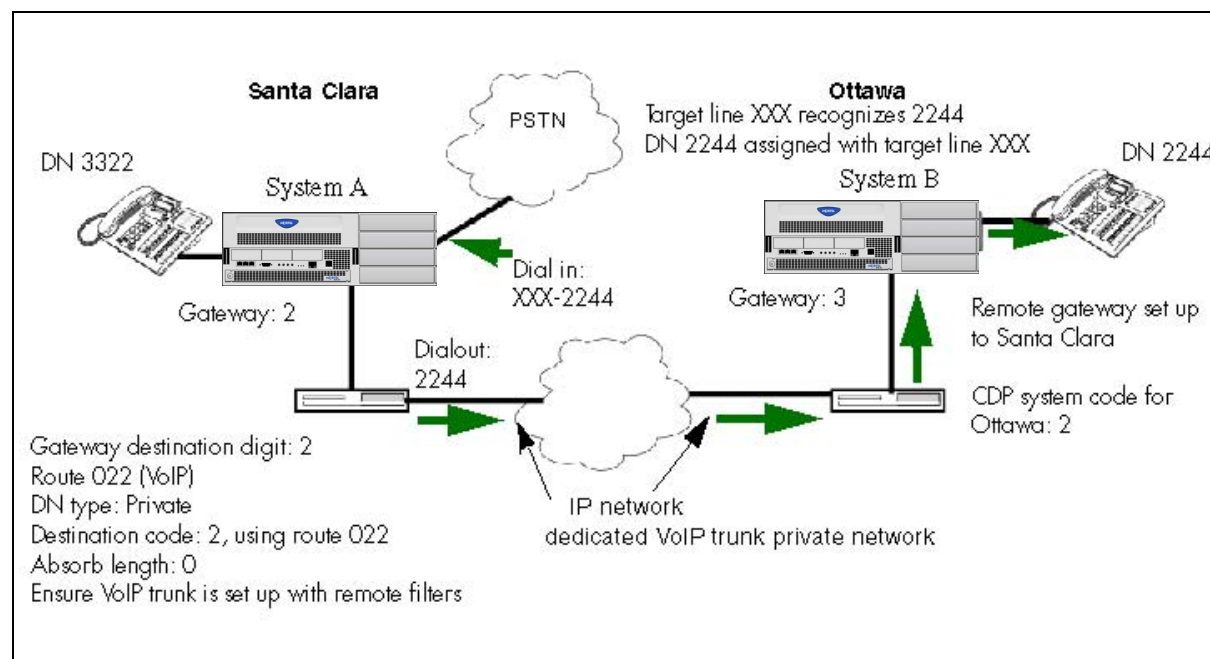
Table 70 T.38 restrictions and requirements

Supported	Not supported
only UDP transport	TCP
only UDP redundancy	Forward Error Correction (FEC)
T.38 version 0	Fill removal
on H.323 VoIP trunks between BCMs, between BCM and legacy BCMs, or between BCM and Meridian 1-IPT and CS 1000/M	MMR transcoding
	JBIG transcoding

Example of call flow, PSTN into remote node

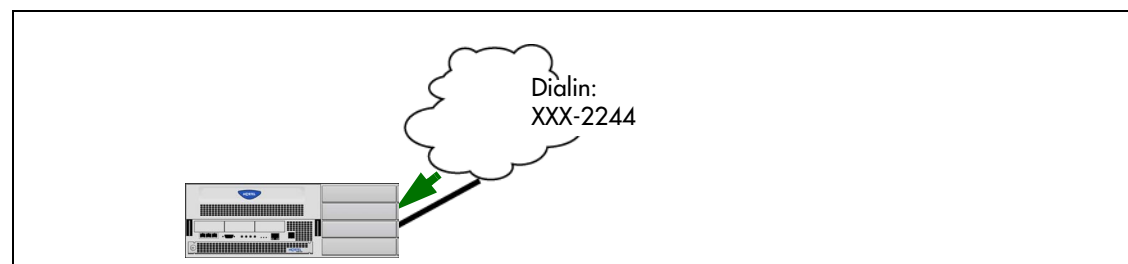
The following figure shows a call tandeming from the public network (PSTN), through System A (Santa Clara) and being passed to System B (Ottawa) over a VoIP trunk network. In this case, it might be a home-based employee who wants to call someone in Ottawa.

Figure 56 Calling into a remote node from a public location



Detail of call progress for example

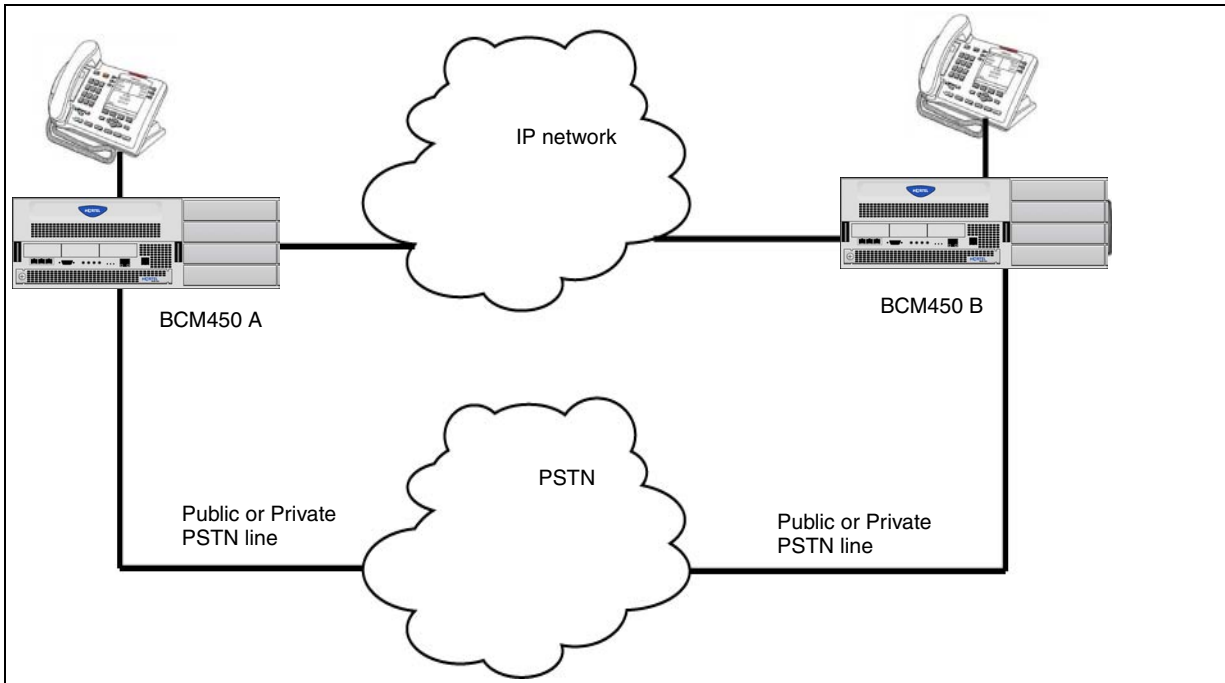
Based on the following figure, this is how the call would progress.



Example of a fallback network

The following figure shows how a fallback network would be set up between two sites.

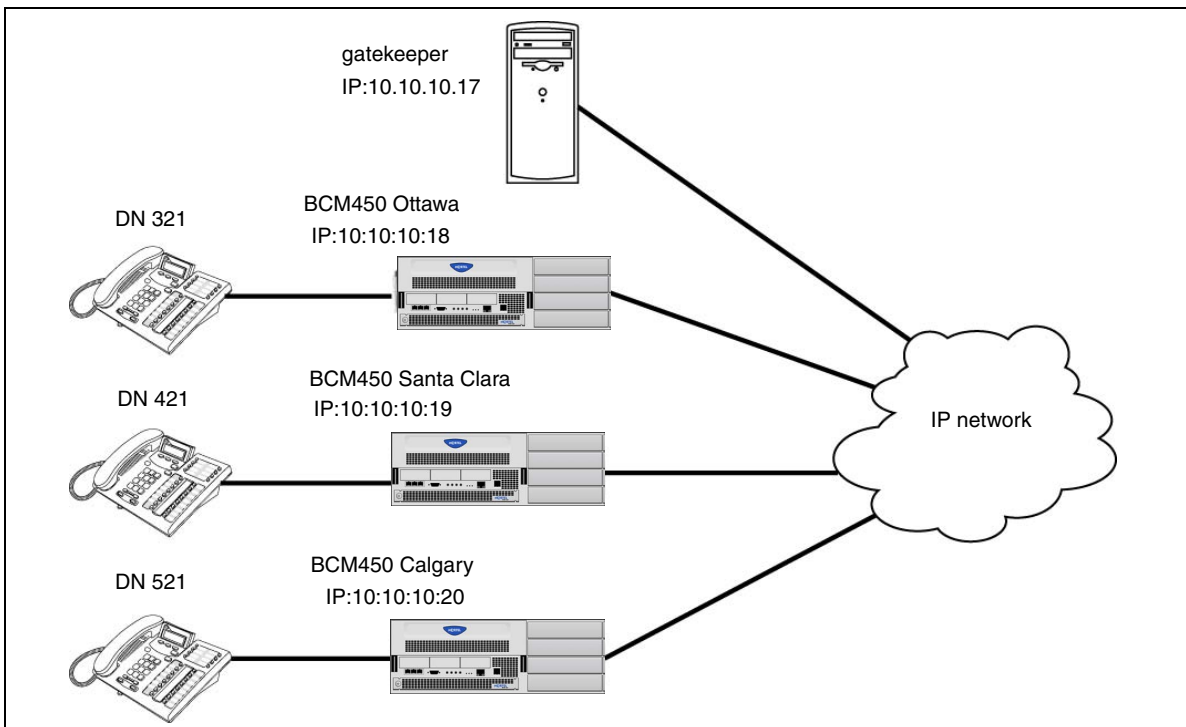
Figure 57 Fallback network diagram



Gatekeeper call scenarios

The following figures show a network with three BCMs and a gatekeeper.

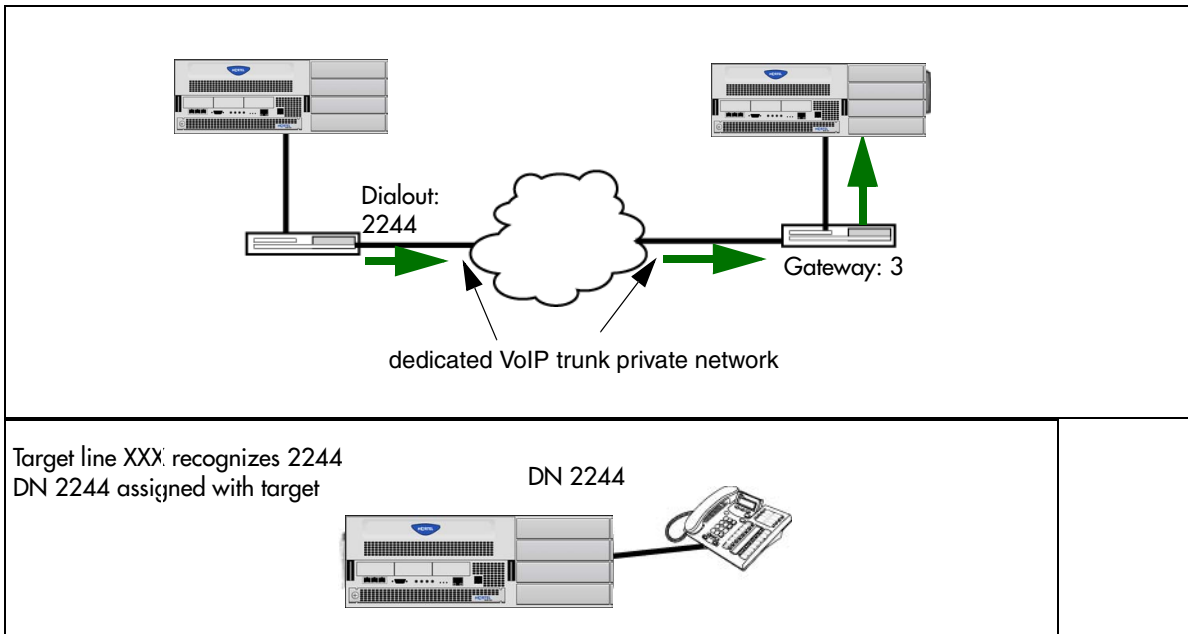
Figure 58 BCM systems with a gatekeeper



Detail of call progression for example

Refer to the following figures for the details of call progression.

Figure 59



SIP fax over G.711 specifications

This feature allows fax to be transmitted using G.711 over SIP trunks in networks that contain SIP endpoint devices that do not support T.38 fax.

Configure IP trunks and gateways before you set up the G.711 fax protocol.

To configure this feature, designate the analog ports to which fax machines are connected as Modem rather than Telephone. This indicates to IP trunks that the bearer capability of these ports is 3.1 K audio.

You can choose between T.38 or G.711 to transmit fax calls over SIP trunks. T.38 and G.711 are mutually exclusive. If you choose G.711 for fax transport, T.38 is not used. If you choose T.38, G.711 is not used. The choice between T.38 and G.711 is made on the SIP Media Parameters panel and applies to all SIP trunk calls.

Both ends of the SIP call are responsible for “listening” for fax tones and configuring their G.711 tasks to transmit and receive fax reliably.

No support is available for tandem G.711 fax calls between H.323 and SIP trunks because H.323 supports only T.38 for transmitting fax.

G.711 Fax restrictions

Fax tones that broadcast through a telephone speaker can disrupt calls on other telephones using VoIP trunks near the fax machine. Follow these suggestions to reduce the chance of your VoIP calls being dropped because of fax tone interference:

- Position the fax machine away from other telephones.
- Turn the speaker volume on the fax machine to the lowest level, or off.

Fax tones can be recorded in a voice mailbox. In the rare event that fax tones are captured in a voice mail message, opening that message from a telephone using a VoIP trunk can cause the connection to fail.

If you allow fax messaging for the local VoIP gateway, you must be aware of the guidelines in [Operational notes and restrictions \(page 290\)](#) when you send and receive fax messages over VoIP trunks. For more information, see [VoIP trunk gateways \(page 173\)](#).

Operational notes and restrictions

Some fax machines cannot successfully send faxes over VoIP trunks to the following destination:

- CallPilot mailboxes
- CallPilot mailboxes accessed through auto-attendant
- Fax Transfer (calls transferred to a system fax device through the auto-attendant)

Use the following tips to avoid this problem:

- Avoid using manual dial on the originating fax machine. In some fax machines, dialing manually results in a much shorter call time-out.
- If you must dial manually, wait until the call is answered before you start the fax session.
- For Mailbox Call Answering only, if you must dial manually, enter the digit 8 as soon as you hear the mailbox greeting. This ensures that CallPilot initiates the fax session before the fax machine timer starts.

Attention: Enter the digit 8 for Norstar Voice Mail User Interface (NVMUI) only. To enable fax call answering when using CallPilot User Interface (CPUI), enter 707.

- Increase the call duration by adding a timed pause to the end of the dialing string. This addition allows the call to ring at the destination before the fax machine call-duration timer starts. Refer to your fax machine documentation for more information on how to insert pauses into dial strings.
- Because the problem is related to the delay in initiating the fax session, reduce the number of rings for fax mailboxes Call Forward No Answer (CFNA).

T.38 fax specifications

This section gives the specification required for the configuration of T.38 fax.

Example of private network configured for T.38 fax

You can assign VoIP trunks to wired fax machines if you have T.38 fax enabled on the local gateway. The BCM supports this IP fax feature between BCMs, BCM200/400 running BCM 4.0, BCM50 3.0, and BCM450 1.0, and subsequent up-level versions of software, and a Meridian 1 running IPT 3.0 (or newer) software, or a CS 1000/M. The system processes fax signals by initiating a voice call over the VoIP line. When the T.38 fax packets are received at the remote gateway, the receiving system establishes a new path that uses the T.38 protocol. Both the endpoints must be running a software version that supports the T.38 fax.



CAUTION

Risk of loss of service.

Fax tones that broadcast through a telephone speaker may disrupt calls at other telephones using VoIP trunks in the vicinity of the fax machine. Here are some suggestions to minimize the possibility of your VoIP calls being dropped because of fax tone interference:

- Locate fax machine away from other telephones.
- Turn the speaker volume on the fax machine to the lowest level, or off.

Fax tones recorded in a voice mailbox: In the rare event that fax tones are captured in a voice mail message, opening.

Programmed Media gateway values for example

Refer the following table for the media gateway values.

Attribute	value	Description
T.38 UDP Redundancy	<numeric character string>	If T.38 fax is enabled on the system, this setting defines how many times the message is resent during a transmission, to avoid errors caused by lost T.38 messages.

Voice messaging specifications

The following table describes each part of the NSI string.

Table 71 Parts of the NSI string

String Component	Description
*58	Identifies that it is an NSI string.
X	Any letter from A to Z, or nothing.
YYYYY.	Manufacturer specific string, which can contain any sequence of alphanumeric digits or *.
#	Marks the end of the identifier.

Default VoIP settings specifications

On the BCM, DHCP can be set up in a variety of configurations, based on your needs, your existing network, and the version of the BCM that you have. For more information on DHCP, refer to [DHCP overview \(page 259\)](#).

BCM450 models

The default DHCP status is assigned to Enabled - IP Phones Only. By default, the BCM is a DHCP client.

Call security and remote access specifications

This section give the specifications for call security and remote access.

Default restriction filters

Refer to the following table for the default restriction filters.

Table 72 Default restriction filters

Filter	Restrictions (denied)	Overrides
00	Unrestricted dialing	
01	01: 0	
	02: 1	02: 1866 001: 1800 002: 1877 003: 1888
	03: 911	001: 911
	04: 411	
	05: 976	
	06: 1976	
	07: 1AAA976	
	08: 1900	
01	09: 1AAA900	
	10: 5551212	
02 - 99	No restrictions or exceptions programmed	

Attention: Default filters are loaded when the system is initialized. A cold start restores the default filters.

Default filters for program headings

Refer to the following table for default filters for program headings.

Table 73 Default filters for program headings

Filter	Heading6	Sub-heading
02	System DNs	Set restrictions
03	Lines	Line restriction
04	Lines	Remote restriction

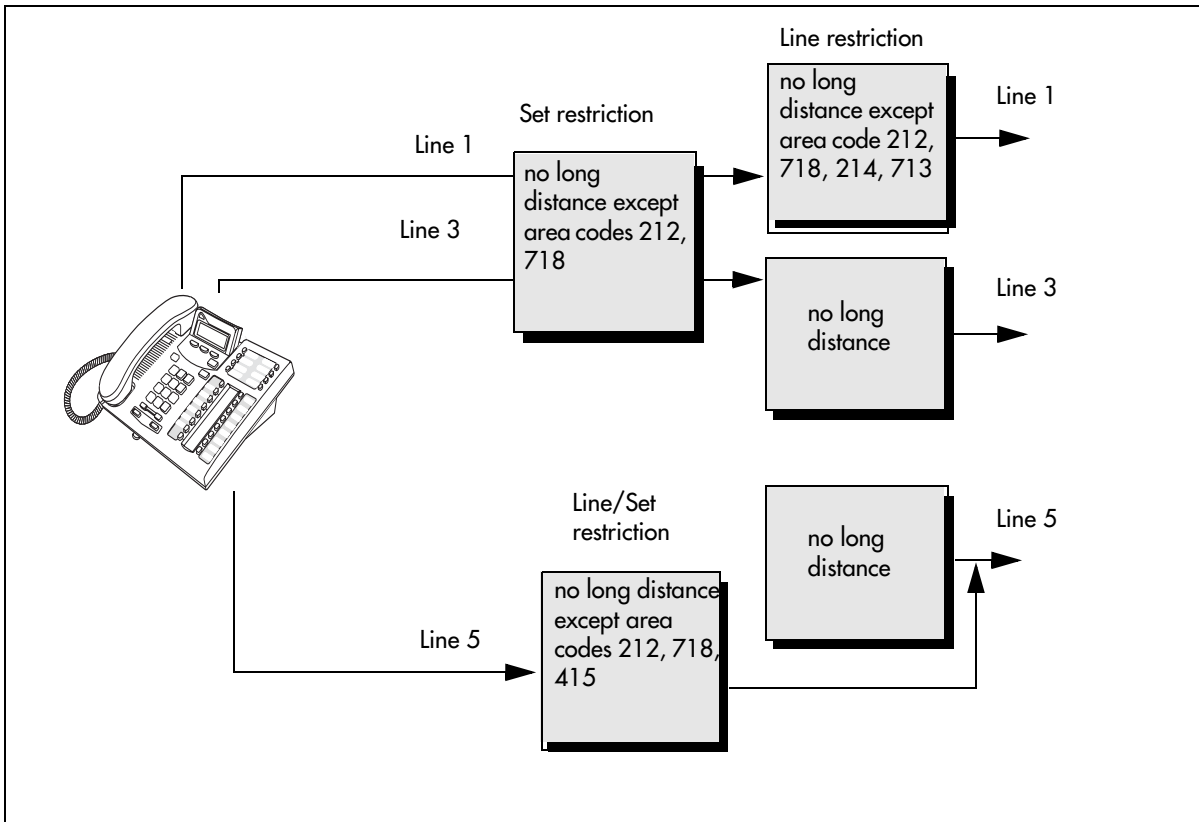
External access tones, definitions

Refer to [External access tones, definitions \(page 298\)](#).

Example of line restriction

An example of line restriction is shown in the following figure.

Figure 60 Line restriction example



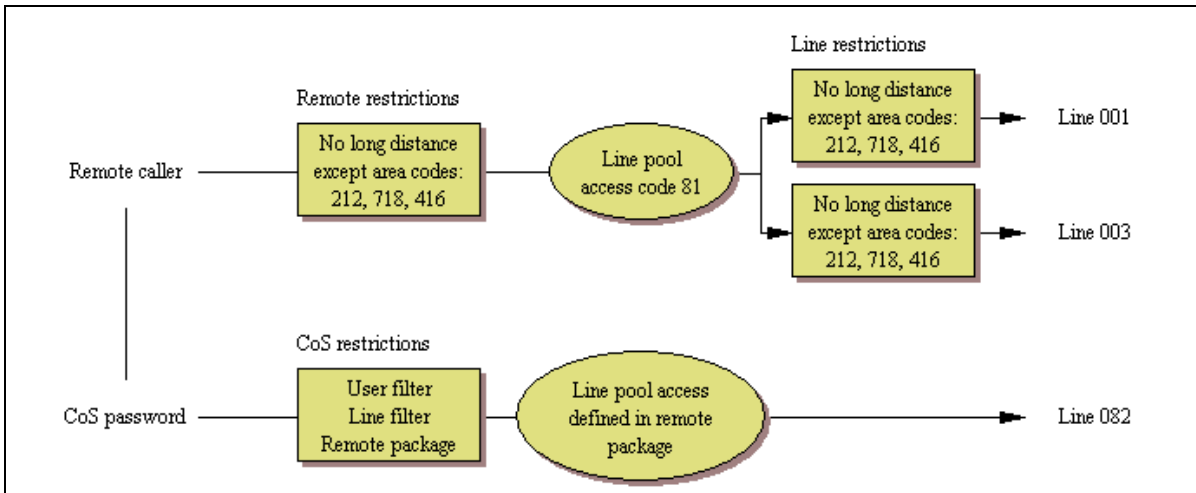
Call progress through restrictions

To restrict dialing from outside the system (once a caller gains remote access), apply restriction filters to incoming external lines (as remote restrictions).

Example of remote line restriction

Refer to the following figure for an example of remote line restriction.

Figure 61 Remote line restriction example



Call progress through restrictions

Dialed digits must pass both the remote restriction and the line restriction. A remote caller can override these filters by dialing the DISA DN and entering a CoS password.

CoS password configuration for remote access specifications

This section gives the specifications of CoS password configuration for remote access.

Example of CoS to access system over PSTN

A sales representative out of the office needs to make long distance calls to the European office. Your system has a leased line to Europe with reduced transatlantic charges. You provide the sales representative with a Class of Service password that gives access to the transatlantic line. The sales representative can telephone into the system (DISA DN) from a hotel, enter the Class of Service password, and then use a destination code to access the leased transatlantic line to make calls.

To use CoS to access system over PSTN carry out the following steps:

- 1 Dial the system remote access number.
- 2 When you hear a stuttered dial tone, enter your CoS password.
- 3 Wait for the system dial tone.

Example of CoS to bypass filters on a set

To use the system at a distance, you must use a telephone with tone dialing to call the system. Remote access is possible only on lines that your installer programs to auto-answer calls. To use paging on a remote system, press * followed by the feature code. When you are calling from within BCM, press * instead of FEATURE. In some conditions, you can experience lower volume levels when using the system from a distance.

To bypass the restriction filters on a telephone carry out the following steps:

- 1 Press **FEATURE 68**.
- 2 Enter the six-digit CoS password that allows the required type of call.
- 3 Enter the number to be dialed.

Dialing plan specifications

This section provides specifications for dialing plan.

Navigation

- [System identification of calls \(page 303\)](#)
- [Default access codes \(page 304\)](#)
- [Tips on using access codes \(page 304\)](#)
- [Protocols that support call-by-call limits \(page 305\)](#)
- [Protocols that support call-by-call limits \(page 305\)](#)
- [Available call-by-call services \(page 305\)](#)
- [Switches supporting call-by-call limits \(page 306\)](#)
- [PRI service type / DN type values for BCM450 \(page 307\)](#)
- [PRI service type / Service ID description \(page 307\)](#)

System identification of calls

How the system identifies the call depends on the type of trunk chosen for the route. Refer to the following table.

Dialing plan setting	NPI/TON	Private called number length based on
MCDN trunks send private calls in this way:		
None	Private/Subscriber	Private DN length (set on Private Network panel)
UDP	Private/UDP	private access code + home location code (LOC) + private received digits
CDP	Private/CDP	private received digit
DMS-100/DMS-250/ETSI-QSIG trunks send private calls in this way:		
None	Private/Subscriber	Private DN length (set on Private Network panel)

Dialing plan setting	NPI/TON	Private called number length based on
UDP	Private/Subscriber	private access code + home location code (LOC) + private received digits
CDP	Private/Subscriber	private received digit

Default access codes

The default settings shown in the following table can help you plan your access codes so that there are no conflicts.

Table 74 Default codes table

Digit	Use	System panel
0	direct dial digit	Access codes
1	park prefix	Access codes
2XX	first digit of DNs/DN lengths	Set through Quick Start Wizard
9	line pool A destination code (Takes precedence over the External line destination code if there is a conflict.)	Routing
Digit	Use	System panel

Tips on using access codes

Here are some pointers to assist you in planning the access codes for your system.

Attention: The following codes/digits must not conflict:
park prefix, external code, direct dial digit, private access code, Public/Private Auto DN, Public/Private DISA DN, line pool code/destination code, telephone DN

Attention: When configuring a private network, ensure the numbering plan does not conflict with the public telephone network. For example, in North America, using “1” as an access code in a private network, conflicts with the PSTN numbering plan for long-distance calls

- **External line access code:** If the DN length is changed, and the changed DNs conflict with the external line access code, the setting changes to None.
- **Direct dial telephone:** Another direct dial telephone, an extra dial telephone, can be assigned for each schedule in Services programming. If the DN length is changed, and the changed DNs conflict with the Direct dial digit, the setting changes to None.

- **Public/Private Auto DN:** The length of the Auto DNs are the same as the Public or Private Received Number Lengths specified under Configuration > Telephony > Dialing Plan. The public/private Auto DN is cleared if the corresponding Received Number Length is changed.
- **Public/Private DISA DN:** The length of the DISA DNs are the same as the Public or Private Received number length specified under Configuration > Telephony > Dialing Plan. The public/private DISA DN is cleared if the corresponding Received number length is changed.

Protocols that support call-by-call limits

The following protocols support call-by-call limits:

- National ISDN 2 (NI-2)
- DMS-100 custom
- DMS-250
- AT&T 4ESS custom

Available call-by-call services

BCM supports the Call-by-Call Services listed in the following table.

Table 75 Call-by-Call Services available on the system

Service	Description
Public	Public calls connect BCM and a Central Office (CO). BCM supports both incoming and outgoing calls over the public network. Dialed digits conform to the standard North American dialing plan (E.164 standard).
Foreign Exchange (FX)	Foreign exchange service connects a BCM site to a remote central office (CO). This provides the equivalent of local service at the remote location.
TIE	TIE lines are private incoming and outgoing lines that connect Private Branch Exchanges (PBXs) such as another BCM.
OUTWATS	Outward Wide Area Telecommunications: This outgoing call service allows a BCM user to call telephones in a specific geographical area referred to as a zone or band. Typically, a flat monthly fee is charged for this service.
INWATS	Inward Wide Area Telecommunications: This long-distance service allows a BCM user to receive calls originating from specified areas without charge to the caller. A toll-free number is assigned to permit reverse billing.
International INWATS	An international long-distance service that allows a BCM user to receive international calls originating from specified areas without charge to the caller. A toll-free number is assigned to permit reverse billing.

Table 75 Call-by-Call Services available on the system

Service	Description
Switched Digital	This service provides premises-to-premises voice and data transport with call management and monitoring features.
Nine Hundred	This service is commonly referred to as fixed-charge dialing.
Private	Private incoming and outgoing calls connect BCM to a virtual private network. Dialed digits can conform to the standard North American dialing plan (E.164 standard) or the dialed digits can use a private dialing plan.

Switches supporting call-by-call limits

The following table lists the service types and cross-references them with four common switches.

Table 76 Switches and service types chart

	Switches			
Service types ¹	NI-2	DMS-100 (custom)	DMS-250	AT&T 4ESS
FX	FX	FX ²	N/A	N/A
Tie ³	TIE	TIE	TIE	SDN (software defined network)
INWATS	INWATS	INWATS	Eight Hundred	Toll Free MEGACOM
International INWATS	Same as INWATS	Same as INWATS	Same as INWATS	International Toll Free Service
OUTWATS	IntraLATA OUTWATS OUTWATS with bands InterLATA OUTWATS	OUTWATS	PRISM	MEGACOM
Private		DMS Private ⁵	VNET (virtual network)	N/A
Switched Digital	N/A	N/A	N/A	ACCUNET ⁴
Nine Hundred	N/A	N/A	Nine Hundred	MultiQuest
Public	Public	Public	Public	N/A
1. N/A indicates that the protocol does not support the service. 2. DMS-250 Sprint and UCS support incoming FX only (that is, Network-to-BCM). DMS-250 MCI does not support FX. 3. NI-2 allows two TIE operating modes: senderized and cut-through. BCM supports only senderized mode. 4. Rates greater than 64 kbps are not supported. 5. Bell Canada VNET. 6. Not all service types may be supported by a switch type. For information, contact your service provider.				

PRI service type / DN type values for BCM450

The following table lists the service/DN type choices available for PRI lines.

Table 77 PRI Service type/DN type values

PRI Protocol	Type	Values
MCDN	DN	Public, Private, Local, International, National, Special
ETSI Euro	DN	Public, Local, International, National
ETSI QSIG	DN	Public, Private, Local, International, National
NI	DN	Public, Private, Local, International, National
ETSI Euro	Service	None, Overlap
NI	Service	Public, TIE, Foreign Exchange (FX), OUTWATS
DMS-100	Service	Public, Private, TIE, Foreign Exchange (FX), OUTWATS
DMS-250	Service	Public, Private, TIE, Foreign Exchange (FX), OUTWATS
4ESS	Service	TIE, OUTWATS, Switched Digital (SDS)

PRI service type / Service ID description

The service identifier (SID) depends on the selected service type (for example, with NI-2 protocol).

Service Type	Service Identifier description
Public	None
FX	Facility Number 1-5 digits
TIE	Facility Number 1-5 digits
OUTWATS ^a	Optional Band Number 1-3 digits
Private	None
Switched Digital	None
a. For NI-2, do not program the Carrier Access Code for banded OUTWAT calls. This call may be rejected.	

Nortel Business Communications Manager 450 1.0

Planning and Engineering

Copyright © 2008 Nortel Networks. The information in this document is sourced in Canada, the United States, India and the United Kingdom.

All Rights Reserved.

Publication: NN40160-200

Document status: Standard

Document issue: 01.01

Document date: August 2008

Product release: BCM450 1.0

Job function: Planning and Engineering

Type: Publication

Language type: EN

NORTEL, the globemark design, and the NORTEL corporate logo are trademarks of Nortel Networks.

To provide feedback or report a problem with this document, go to www.nortel.com/document feedback.

